HIGHER NEWTON POLYGONS AND INTEGRAL BASES

JORDI GUÀRDIA, JESÚS MONTES, AND ENRIC NART

Abstract. Let A be a Dedekind domain whose field of fractions K is a global field. Let $\mathfrak{p}$ be a non-zero prime ideal of A, and $K_{\mathfrak{p}}$ the completion of K at $\mathfrak{p}$. The Montes algorithm factorizes a monic irreducible separable polynomial $f(x) \in A[x]$ over $K_{\mathfrak{p}}$, and it provides essential arithmetic information about the finite extensions of $K_{\mathfrak{p}}$ determined by the different irreducible factors. In particular, it can be used to compute a $\mathfrak{p}$-integral basis of the extension of K determined by $f(x)$. In this paper we present a new and faster method to compute $\mathfrak{p}$-integral bases, based on the use of the quotients of certain divisions with remainder of $f(x)$ that occur along the flow of the Montes algorithm.

Introduction

Let A be a Dedekind domain whose field of fractions K is a global field. Let $\mathfrak{p}$ be a non-zero prime ideal of A, and $\pi \in A$ a local generator of $\mathfrak{p}$. Let $K_{\mathfrak{p}}$ be the completion of K with respect to the $\mathfrak{p}$-adic topology.

Let $f(x) \in A[x]$ be a monic irreducible separable polynomial of degree n. Let $\theta \in K^{\rm sep}$ be a root of $f(x)$, $L = K(\theta)$ be the finite separable extension of K generated by θ, and B be the integral closure of A in L.

The Montes algorithm [6, 7] computes an *OM representation* of every prime ideal $\mathfrak{P}$ of B lying over $\mathfrak{p}$ [8]. This algorithm carries out a program suggested by Ø. Ore [18] and developed by S. MacLane in the context of valuation theory [14, 15]. An OM representation is a computational object supporting several data and operators, linked to one of the irreducible factors (say) $F(x)$ of $f(x)$ in $K_{\mathfrak{p}}[x]$. Among these data the *Okutsu invariants* of F stand out, revealing a lot of arithmetic information about the finite extension of $K_{\mathfrak{p}}$ determined by F [16, 5]. The initials OM stand indistinctly for Ore-MacLane or Okutsu-Montes.

In [8] we presented a method to compute $\mathfrak{p}$-integral bases of B/A, based on these OM representations of the prime ideals of B dividing $\mathfrak{p}$. For n large, this method is significantly faster than the traditional methods, most of them based on variants of the Round 2 and Round 4 routines [2, 3, 4, 10, 12, 19, 23].

In this paper we present an improvement of that OM-method, based on the use of *quotients of ϕ-adic expansions*. This idea goes back to a construction of integral bases by W.M. Schmidt for certain subrings of function fields [20]. Along the flow of the Montes algorithm, some polynomials $\phi(x) \in A[x]$ are constructed as a kind of optimal approximations to the irreducible factors of $f(x)$ over $K_{\mathfrak{p}}$. The (conveniently truncated) ϕ-expansions of $f(x)$ provide the necessary data to build higher order Newton polygons of $f(x)$, from which new and better approximations

2010 *Mathematics Subject Classification.* Primary 11R04; Secondary 11Y40, 14G15, 14H05.

Key words and phrases. Dedekind domain, global field, local field, Montes algorithm, Newton polygon, p-integral bases, reduced bases.

Partially supported by MTM2009-10359 and MTM2012-34611 from the Spanish MEC.

are deduced. As a by-product of the computation of any ϕ-expansion, $f(x) = \sum_{0\le s} a_s(x)\phi(x)^s$, we obtain several quotients:

$$f(x) = \phi(x)Q_1(x) + a_0(x), \quad Q_1(x) = \phi(x)Q_2(x) + a_1(x), \quad \dots$$

These polynomials $Q_i(x)$ have nice properties that can be exploited to obtain shortcuts and improvements in the computation of $\mathfrak{p}$-integral bases.

The outline of the paper is as follows. In section 1 we review the main technical ingredients of the paper: OM representations and Okutsu invariants of irreducible separable polynomials over local fields. In section 2 we review the OM-method of [8] for the computation of integral bases. In section 3, we study the quotients $Q(x)$ obtained along the computation of ϕ-expansions of $f(x)$. We analyze the $\mathfrak{P}$-adic value of $Q(\theta)$, for all prime ideals $\mathfrak{P}$ lying over $\mathfrak{p}$, in order to determine the highest exponent μ such that $Q(\theta)/\pi^\mu$ is $\mathfrak{p}$-integral (Theorem 3.3 and Corollary 3.7). In section 4, we show how to construct local bases with these quotients. For every prime ideal $\mathfrak{P} \mid \mathfrak{p}$, we find a family of elements of L whose images in the $\mathfrak{P}$-completion $L_\mathfrak{P}$ are an integral basis of the local extension $L_\mathfrak{P}/K_\mathfrak{p}$. These elements are constructed as a product of quotients, divided by an adequate power of π. The essential difference with the OM-method is that all these elements are already $\mathfrak{p}$-integral (globally integral if A is a PID), and not only $\mathfrak{P}$-integral. Finally, in section 5 we show how to use these $\mathfrak{p}$-integral elements to build a $\mathfrak{p}$-integral basis (Theorem 5.16). This *method of the quotients* has three significant advantages with respect to the former OM-method and all classical methods:

(1) It yields $\mathfrak{p}$-*reduced* bases. For instance, let $L = \mathbb{F}(t, x)$ be the function field of a curve C over a finite field $\mathbb{F}$, defined by an equation $f(t, x) = 0$, which is separable over $K = \mathbb{F}(t)$. For the subring $A = \mathbb{F}[t^{-1}]$ and the prime ideal $\mathfrak{p} = t^{-1}A$, a $\mathfrak{p}$-reduced basis of B/A is just a classical reduced basis with respect to a certain size function determined by the degree function on A [13, Sec. 16]. The construction of reduced bases is a key ingredient in the computation of bases of the Riemann-Roch spaces attached to divisors of C [20], [22], [11].

(2) It admits a neat complexity analysis (Theorem 6.2). The method requires only $O(n)$ multiplications in the ring $A[\theta]$, along an ordinary application of the Montes algorithm with input data $(f(x), \mathfrak{p})$. If $A/\mathfrak{p}$ is small, the computation of a $\mathfrak{p}$-integral basis requires altogether $O\left(n^{2+\epsilon}\delta^{1+\epsilon} + n^{1+\epsilon}\delta^{2+\epsilon}\right)$ word operations, where δ is the $\mathfrak{p}$-adic valuation of the discriminant of $f(x)$.

(3) It has an excellent practical performance. For $A = \mathbb{Z}$, the method may be tested by running the `pIntegralBasis` routine of the Magma package `+Ideals.m`, which may be downloaded from the site `http://www-ma4.upc.edu/~guardia/+Ideals.html`.

1. Okutsu invariants of irreducible polynomials over local fields

Let k be a local field, i.e. a locally compact and complete field with respect to a discrete valuation v. Let $\mathcal{O}$ be the valuation ring of k, $\mathfrak{m}$ the maximal ideal, $\pi \in \mathfrak{m}$ a generator of $\mathfrak{m}$ and $\mathbb{F} = \mathcal{O}/\mathfrak{m}$ the residue field, which is a finite field.

Let $k^{\rm sep} \subset \overline{k}$ be the separable closure of k inside a fixed algebraic closure. Let $v\colon \overline{k} \to \mathbb{Q} \cup \{\infty\}$, be the canonical extension of the discrete valuation v to $\overline{k}$, normalized by $v(k) = \mathbb{Z}$.

Let $F(x) \in \mathcal{O}[x]$ be a monic irreducible separable polynomial, $\theta \in k^{\text{sep}}$ a root of $F(x)$, and $L = k(\theta)$ the finite separable extension of k generated by θ. Denote $n := [L\colon k] = \deg F$. Let $\mathcal{O}_L$ be the ring of integers of L, $\mathfrak{m}_L$ the maximal ideal and $\mathbb{F}_L$ the residue field. We indicate with a bar, $\overline{}\colon \mathcal{O}[x] \longrightarrow \mathbb{F}[x]$, the canonical homomorphism of reduction of polynomials modulo $\mathfrak{m}$.

Let $[\phi_1, \dots, \phi_r]$ be an *Okutsu frame* of $F(x)$, and let ϕ_{r+1} be an *Okutsu approximation* to $F(x)$. That is, $\phi_1, \dots, \phi_{r+1} \in \mathcal{O}[x]$ are monic separable polynomials of strictly increasing degree:

$$1 \le m_1 := \deg \phi_1 < \cdots < m_r := \deg \phi_r < m_{r+1} := \deg \phi_{r+1} = n,$$

and for any monic polynomial $g(x) \in \mathcal{O}[x]$ we have:

$$\deg g < m_{i+1} \implies \frac{v(g(\theta))}{\deg g} \le \frac{v(\phi_i(\theta))}{m_i} < \frac{v(\phi_{i+1}(\theta))}{m_{i+1}}, \tag{1}$$

for $0 \le i \le r$, with the convention that $m_0 = 1$ and $\phi_0(x) = 1$. It is easy to deduce from (1) that the polynomials $\phi_1(x), \dots, \phi_{r+1}(x)$ are all irreducible in $\mathcal{O}[x]$.

The length r of the frame is called the *Okutsu depth* of $F(x)$. We have $r = 0$ if and only if $\overline{F}$ is irreducible over $\mathbb{F}$; in this case, the Okutsu frame is an empty list. Okutsu frames were introduced by K. Okutsu in [16] as a tool to construct integral bases. Okutsu approximations were introduced in [5], where it is shown that the family $\phi_1, \dots, \phi_{r+1}$ determines an *optimal F-complete type of order $r+1$*:

$$\mathbf{t}_F = (\psi_0; (\phi_1, \lambda_1, \psi_1); \cdots; (\phi_r, \lambda_r, \psi_r); (\phi_{r+1}, \lambda_{r+1}, \psi_{r+1})). \tag{2}$$

In the special case $\phi_{r+1} = F$, we have $\lambda_{r+1} = -\infty$ and ψ_{r+1} is not defined. We call $\mathbf{t}_F$ an *OM representation* of F.

Any OM representation of the polynomial F carries (stores) several invariants and operators yielding strong arithmetic information about F and the extension L/k. Let us recall some of these invariants and operators.

Attached to the type $\mathbf{t}_F$, there is a family of discrete valuations of the rational function field $k(x)$, the *MacLane valuations*:

$$v_i\colon k(x) \longrightarrow \mathbb{Z} \cup \{\infty\}, \quad 1 \le i \le r+1,$$

satisfying $0 = v_1(F) < \cdots < v_{r+1}(F)$. The v_1-value of a polynomial in $k[x]$ is the minimum of the v-values of its coefficients.

Also, $\mathbf{t}_F$ determines a family of Newton polygon operators:

$$N_i\colon k[x] \longrightarrow 2^{\mathbb{R}^2}, \quad 1 \le i \le r+1,$$

where $2^{\mathbb{R}^2}$ is the set of subsets of the Euclidean plane. Any non-zero polynomial $g(x) \in k[x]$ has a canonical ϕ_i-development:

$$g(x) = \sum\nolimits_{0 \le s} a_s(x) \phi_i(x)^s, \quad \deg a_s < m_i,$$

and the polygon $N_i(g)$ is the lower convex hull of the set of points $(s, v_i(a_s \phi_i^s))$. Usually, we are only interested in the principal polygon $N_i^-(g) \subset N_i(g)$ formed by the sides of negative slope. For all $1 \le i \le r$, the Newton polygons $N_i(F)$ and $N_i(\phi_{i+1})$ are one-sided and they have the same slope, which is a negative rational number $\lambda_i \in \mathbb{Q}_{<0}$. The Newton polygon $N_{r+1}(F)$ is one-sided and it has an (extended) integer negative slope, which we denote by $\lambda_{r+1} \in \mathbb{Z}_{<0} \cup \{-\infty\}$.

There is a chain of finite extensions: $\mathbb{F} = \mathbb{F}_0 \subset \mathbb{F}_1 \subset \cdots \subset \mathbb{F}_{r+1} = \mathbb{F}_L$. The type $\mathbf{t}_F$ stores monic irreducible polynomials $\psi_i(y) \in \mathbb{F}_i[y]$ such that $\mathbb{F}_{i+1} \simeq$

$\mathbb{F}_i[y]/(\psi_i(y))$. We have $\psi_i(y) \neq y$, for all $i > 0$. Finally, for every negative rational number λ, there are *residual polynomial* operators:

$$R_{\lambda,i}\colon k[x] \longrightarrow \mathbb{F}_i[y], \quad 0 \leq i \leq r+1.$$

We define $R_i := R_{\lambda_i,i}$. For all $0 \leq i \leq r$, we have $R_i(F) = \psi_i^{\omega_{i+1}}$ and $R_i(\phi_{i+1}) = \psi_i$. The exponents ω_{i+1} are all positive and $\omega_{r+1} = 1$. The operator R_{r+1} is defined only when $\phi_{r+1} \neq F$; in this case, we also have $R_{r+1}(F) = \psi_{r+1}$, with $\psi_{r+1}(y) \in \mathbb{F}_{r+1}[y]$ monic of degree one such that $\psi_{r+1}(y) \neq y$.

From these data some more numerical invariants are deduced. Initially we take:

$$m_0 := 1, \quad f_0 := \deg \psi_0, \quad e_0 := 1, \quad h_0 := V_0 = 0.$$

Then, we define for all $1 \leq i \leq r+1$:

$$\begin{aligned}
&h_i,\, e_i \ \text{ positive coprime integers such that } \lambda_i = -h_i/e_i,\\
&f_i := \deg \psi_i,\\
&m_i := \deg \phi_i = e_{i-1}f_{i-1}m_{i-1} = (e_0\, e_1 \cdots e_{i-1})(f_0 f_1 \cdots f_{i-1}),\\
&V_i := v_i(\phi_i) = e_{i-1}f_{i-1}(e_{i-1}V_{i-1} + h_{i-1}),\\
&\ell_i,\, \ell_i' \ \text{ a pair of integers such that } \ell_i h_i - \ell_i' e_i = 1,\\
&z_{i-1} := \ \text{the class of } y \text{ in } \mathbb{F}_i, \text{ so that } \psi_{i-1}(z_{i-1}) = 0.
\end{aligned}$$

An irreducible polynomial F admits infinitely many different OM representations. However, the numerical invariants e_i, f_i, h_i, for $0 \leq i \leq r$, and the MacLane valuations $v_1, \ldots, v_{r+1}$ attached to $\mathbf{t}_F$, are canonical invariants of F.

The data $\lambda_{r+1}, \psi_{r+1}$ are not invariants of F; they depend on the choice of the Okutsu approximation ϕ_{r+1}. The integer slope $\lambda_{r+1} = -h_{r+1}$ measures how close is ϕ_{r+1} to F. We have $\phi_{r+1} = F$ if and only if $h_{r+1} = \infty$.

Definition 1.1. *An* Okutsu invariant *of $F(x)$ is a rational number that depends only on $e_0, e_1, \ldots, e_r, f_0, f_1, \ldots, f_r, h_1, \ldots, h_r$.*

For instance, the ramification index and residual degree of L/k are Okutsu invariants of F. More precisely,

$$e(L/k) = e_0 e_1 \cdots e_r, \quad f(L/k) = f_0 f_1 \cdots f_r.$$

The general definition of a *type* may be found in [7, Sec. 2.1]. In later sections, we shall consider types which are not necessarily optimal nor F-complete. So, it may be convenient to distinguish these two properties among all features of a type that we have just described.

Definition 1.2. *Let $\mathbf{t} = (\psi_0; (\phi_1, \lambda_1, \psi_1); \cdots; (\phi_i, \lambda_i, \psi_i))$ be a type of order i and denote $m_{i+1} := e_i f_i m_i$. Let $g(x), h(x) \in k[x]$ be non-zero polynomials.*

• *We say that* $\mathbf{t}$ *is* optimal *if $m_1 < \cdots < m_i$. We say that* $\mathbf{t}$ *is* strongly optimal *if $m_1 < \cdots < m_i < m_{i+1}$.*

• *We define* $\operatorname{ord}_{\mathbf{t}}(g) := \operatorname{ord}_{\psi_i} R_i(g)$ *in* $\mathbb{F}_i[y]$. *If* $\operatorname{ord}_{\mathbf{t}}(g) > 0$, *we say that* $\mathbf{t}$ divides $g(x)$, *and we write* $\mathbf{t} \mid g(x)$. *We have* $\operatorname{ord}_{\mathbf{t}}(gh) = \operatorname{ord}_{\mathbf{t}}(g) + \operatorname{ord}_{\mathbf{t}}(h)$.

• *We say that* $\mathbf{t}$ *is* g-complete *if* $\operatorname{ord}_{\mathbf{t}}(g) = 1$.

• *A* representative *of* $\mathbf{t}$ *is a monic polynomial $\phi(x) \in \mathcal{O}[x]$ of degree m_{i+1}, such that $R_i(\phi) \sim \psi_i$. The degree m_{i+1} is minimal among all polynomials satisfying this condition, and ϕ is necessarily irreducible in $\mathcal{O}[x]$. The choice of a representative of*

$\mathbf{t}$ *determines a Newton polygon operator* $N_{\phi,v_{i+1}}$ *depending on* ϕ *and the valuation* v_{i+1} *supported by* $\mathbf{t}$. *Usually, we denote* $\phi_{i+1} := \phi$ *and* $N_{i+1} := N_{\phi_{i+1},v_{i+1}}$.

• *For any* $0 \le j \le i$, *the* truncation *of* $\mathbf{t}$ *at level* j, $\mathrm{Trunc}_j(\mathbf{t})$, *is the type of order* j *obtained from* $\mathbf{t}$ *by dropping all levels higher than* j.

For a general type of order i dividing F, we have $m_1 \mid \cdots \mid m_i$ and $\omega_i > 0$, but not necessarily $m_1 < \cdots < m_i = \deg F$, and $\omega_i = 1$. These were particular properties of the optimal and F-complete type $\mathbf{t}_F$ of order $i = r+1$, constructed from an Okutsu frame and an Okutsu approximation to F.

Definition 1.3. *The* length *of a Newton polygon* N *is the abscissa of its right end point; we denote it by* $\ell(N)$.

Lemma 1.4. [7, Lem. 2.17,(2)] *Let* $\mathbf{t}$ *be a type of order* $i \ge 0$, *and let* $\phi_{i+1} \in \mathcal{O}[x]$ *be a representative of* $\mathbf{t}$. *Then,* $\ell(N^-_{i+1}(g)) = \mathrm{ord}_{\mathbf{t}}(g)$ *for any non-zero* $g(x) \in k[x]$.

We shall frequently use the following result, extracted from [7, Prop. 3.5,(5)]. Note that it contains the definition of the MacLane valuation v_{i+1}.

Proposition 1.5. *Let* $\mathbf{t}$ *be a type of order* $i \ge 1$, *and let* $F(x) \in \mathcal{O}[x]$ *be a monic irreducible separable polynomial such that* $\mathbf{t} \mid F$. *Let* $\theta \in k^{\mathrm{sep}}$ *be a root of* $F(x)$, *and* $g(x) \in \mathcal{O}[x]$ *a non-zero polynomial. Take a line of slope* λ_i *far below* $N_i(g)$, *and shift it upwards till it touches the polygon for the first time. Let* $(0, H)$ *be the intersection point of this line with the vertical axis. Then,*

$$v(g(\theta)) \ge v_{i+1}(g)/(e_0 \cdots e_i) = H/(e_0 \cdots e_{i-1}),$$

and equality holds if and only if $\mathbf{t} \nmid g(x)$.

Corollary 1.6. *With the above notation,* $v(\phi_j(\theta)) = (V_j + |\lambda_j|)/(e_0 \cdots e_{j-1})$, *for all* $1 \le j \le i$.

Local integral bases. The next result is an elementary combinatorial fact.

Lemma 1.7. *For* $0 \le i \le r$, *consider positive integers* $m_i \mid \cdots \mid m_{r+1}$. *Then, any integer* $0 \le N < (m_{r+1}/m_i)$ *can be expressed in a unique way as:*

$$N = j_i + j_{i+1}(m_{i+1}/m_i) + \cdots + j_r(m_r/m_i),$$

for integers j_k *such that* $0 \le j_k < (m_{k+1}/m_k)$ *for all* $i \le k \le r$.

Let $m_1, \ldots, m_{r+1} = n$ be the degrees of the Okutsu polynomials of an OM representation $\mathbf{t}_F$ of a monic irreducible separable polynomial $F \in \mathcal{O}[x]$, as in (2). Recall that $m_0 = 1$ and $m_{k+1}/m_k = e_k f_k$ for all $0 \le k \le r$. For any integer $0 \le m < n$, consider the following monic polynomial $g_m(x) \in \mathcal{O}[x]$ of degree m:

$$g_m(x) := \prod\nolimits_{0 \le k \le r} \phi_k(x)^{j_k}, \quad m = \sum\nolimits_{0 \le k \le r} j_k m_k, \;\; 0 \le j_k < e_k f_k,$$

where now $\phi_0(x) := x$. Corollary 1.6 provides concrete formulas for all $v(\phi_k(\theta))$; thus, we can easily compute $\mu_m := \lfloor v(g_m(\theta)) \rfloor$ for all m.

Theorem 1.8 (Okutsu, [16, I,Thm. 1])**.** *The following family is an* $\mathcal{O}$*-basis of* $\mathcal{O}_L$*:*

$$1, \; g_1(\theta)/\pi^{\mu_1}, \; \ldots, \; g_{n-1}(\theta)/\pi^{\mu_{n-1}}.$$

The *exponent* of F is the least non-negative integer $\exp(F)$ such that $\pi^{\exp(F)}\mathcal{O}_L$ is included in $\mathcal{O}[\theta]$. Since $\mu_1 \le \cdots \le \mu_{n-1}$, it is clear that $\exp(F) = \mu_{n-1}$.

2. An OM method to compute $\mathfrak{p}$-integral bases

Let A be a Dedekind domain whose field of fractions K is a global field, and let $K^{\rm sep}$ be a separable closure of K. Let $f(x) \in A[x]$ be a monic irreducible and separable polynomial of degree $n > 1$. Let $L = K(\theta)$ be the finite separable extension of K generated by a root $\theta \in K^{\rm sep}$ of $f(x)$. The integral closure $B \subset L$ of A in L is a Dedekind domain too.

Let $\mathfrak{p}$ be a non-zero prime ideal of A. Let $A_{\mathfrak{p}}$ be the localization of A at $\mathfrak{p}$, $\pi \in A$ a generator of the principal ideal $\mathfrak{p}A_{\mathfrak{p}}$, and $\mathbb{F}_{\mathfrak{p}} := A/\mathfrak{p}$ the residue field. The integral closure $B_{\mathfrak{p}}$ of $A_{\mathfrak{p}}$ in L is the subring of $\mathfrak{p}$-integral elements of L:

$$B_{\mathfrak{p}} = \{\alpha \in L \mid v_{\mathfrak{P}}(\alpha) \geq 0,\ \forall \mathfrak{P} \in \mathrm{Spec}(B),\ \mathfrak{P} \mid \mathfrak{p}\},$$

where $v_{\mathfrak{P}}$ is the discrete valuation of L attached to $\mathfrak{P}$. The ring $B_{\mathfrak{p}}$ is a free $A_{\mathfrak{p}}$-module of rank n.

Definition 2.1. *A $\mathfrak{p}$-integral basis of B/A is a family $\alpha_1, \ldots, \alpha_n \in B_{\mathfrak{p}}$, that satisfies any of the following equivalent conditions:*

(a) *$\alpha_1, \ldots, \alpha_n$ is an $A_{\mathfrak{p}}$-basis of $B_{\mathfrak{p}}$.*
(b) *$\alpha_1 \otimes 1, \ldots, \alpha_n \otimes 1$ is an $\mathbb{F}_{\mathfrak{p}}$-basis of $B_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} \mathbb{F}_{\mathfrak{p}} \simeq B_{\mathfrak{p}}/\mathfrak{p}B_{\mathfrak{p}} \simeq B/\mathfrak{p}B$.*

Conditions (a) and (b) are equivalent by Nakayama's lemma. Since $B/\mathfrak{p}B$ has dimension n as an $\mathbb{F}_{\mathfrak{p}}$-vector space, in order to show that $\alpha_1, \ldots, \alpha_n \in B_{\mathfrak{p}}$ form a $\mathfrak{p}$-integral basis of B/A it suffices to check that these elements yield $\mathbb{F}_{\mathfrak{p}}$-linearly independent elements in the $\mathbb{F}_{\mathfrak{p}}$-algebra $B/\mathfrak{p}B$.

Consider the factorization of $\mathfrak{p}B$ into a product of prime ideals in L:

$$\mathfrak{p}B = \mathfrak{P}_1^{e(\mathfrak{P}_1/\mathfrak{p})} \cdots \mathfrak{P}_g^{e(\mathfrak{P}_g/\mathfrak{p})}.$$

Let $K_{\mathfrak{p}}$, $L_{\mathfrak{P}}$, be the completions of K and L with respect to the $\mathfrak{p}$-adic and $\mathfrak{P}$-adic topology, respectively. Denote the ring of integers of these fields by:

$$\mathcal{O}_{\mathfrak{p}} \subset K_{\mathfrak{p}}, \qquad \mathcal{O}_{\mathfrak{P}} \subset L_{\mathfrak{P}},\ \forall \mathfrak{P} \mid \mathfrak{p}.$$

Finally, we denote the local degrees by $n_{\mathfrak{P}} := [L_{\mathfrak{P}} \colon K_{\mathfrak{p}}] = e(\mathfrak{P}/\mathfrak{p})f(\mathfrak{P}/\mathfrak{p})$.

By a classical theorem of Hensel, these prime ideals are in 1-1 correspondence with the different monic irreducible factors of $f(x)$ in $\mathcal{O}_{\mathfrak{p}}[x]$.

Definition 2.2. *For each prime ideal $\mathfrak{P} \mid \mathfrak{p}$, let us fix a topological embedding, $i_{\mathfrak{P}} \colon L \subset L_{\mathfrak{P}} \hookrightarrow \overline{K}_{\mathfrak{p}}$. Then $\theta_{\mathfrak{P}} := i_{\mathfrak{P}}(\theta)$ is the root of a unique monic irreducible factor (say) $F_{\mathfrak{P}}(x)$ of $f(x)$ over $\mathcal{O}_{\mathfrak{p}}$. Also, we denote:*

$$w_{\mathfrak{P}} := e(\mathfrak{P}/\mathfrak{p})^{-1} v_{\mathfrak{P}} \colon L^* \longrightarrow e(\mathfrak{P}/\mathfrak{p})^{-1}\mathbb{Z}.$$

Clearly, $w_{\mathfrak{P}}(\alpha) = v(i_{\mathfrak{P}}(\alpha))$ for all $\alpha \in L$, where $v := v_{\mathfrak{p}}$ is the canonical extension of $v_{\mathfrak{p}}$ to $\overline{K}_{\mathfrak{p}}$. Thus, for any polynomial $g(x) \in A[x]$,

$$w_{\mathfrak{P}}(g(\theta)) = v(g(\theta_{\mathfrak{P}})).$$

This identity will be implicitly used throughout the paper without further mention, when we apply local results to a global situation.

The Montes algorithm provides a family of OM representations of the irreducible factors of $f(x)$ in $\mathcal{O}_{\mathfrak{p}}[x]$. For any prime ideal $\mathfrak{P}$ dividing $\mathfrak{p}$, let us denote by

$$\mathbf{t}_{\mathfrak{P}} := \mathbf{t}_{F_{\mathfrak{P}}} = \left(\psi_{0,\mathfrak{P}}; (\phi_{1,\mathfrak{P}}, \lambda_{1,\mathfrak{P}}, \psi_{1,\mathfrak{P}}); \cdots; (\phi_{r_{\mathfrak{P}}+1,\mathfrak{P}}, \lambda_{r_{\mathfrak{P}}+1,\mathfrak{P}}, \psi_{r_{\mathfrak{P}}+1,\mathfrak{P}})\right),$$

the OM representation corresponding to $F_{\mathfrak{P}}$. All polynomials $\phi_{i,\mathfrak{P}}$ have coefficients in A. The type $\mathbf{t}_{\mathfrak{P}}$ singles out $\mathfrak{P}$ (or $F_{\mathfrak{P}}$) by:

$$\mathbf{t}_{\mathfrak{P}} \mid F_{\mathfrak{P}}, \quad \mathbf{t}_{\mathfrak{P}} \nmid F_{\mathfrak{Q}}, \quad \forall\, \mathfrak{Q} \mid \mathfrak{P},\ \mathfrak{Q} \neq \mathfrak{P}.$$

As we saw in the last section, from the OM representation we derive a family of $\mathfrak{P}$-integral elements in L,

$$\mathcal{B}_{\mathfrak{P}} = \left\{1,\ g_{1,\mathfrak{P}}(\theta)/\pi^{\mu_{1,\mathfrak{P}}},\ \ldots,\ g_{n_{\mathfrak{P}}-1,\mathfrak{P}}(\theta)/\pi^{\mu_{n_{\mathfrak{P}}-1,\mathfrak{P}}}\right\} \subset L.$$

whose image under $i_{\mathfrak{P}}$ is the Okutsu basis of $\mathcal{O}_{\mathfrak{P}}$ as an $\mathcal{O}_{\mathfrak{p}}$-module described in Theorem 1.8. It is easy to build a $\mathfrak{p}$-integral basis with these local $\mathfrak{P}$-bases.

Theorem 2.3 (Ore [17])**.** *For each prime ideal $\mathfrak{P} \mid \mathfrak{p}$, take $\beta_{\mathfrak{P}} \in B_{\mathfrak{p}}$ such that:*

$$w_{\mathfrak{P}}(\beta_{\mathfrak{P}}) = 0, \quad w_{\mathfrak{Q}}(\beta_{\mathfrak{P}}) \geq \exp(F_{\mathfrak{P}}) + 1,\ \forall\, \mathfrak{Q} \mid \mathfrak{p},\ \mathfrak{Q} \neq \mathfrak{P}.$$

Then, $\mathcal{B} := \bigcup_{\mathfrak{P}\mid\mathfrak{p}} \beta_{\mathfrak{P}}\mathcal{B}_{\mathfrak{P}}$ is a $\mathfrak{p}$-integral basis.

In [8, Secs. 4.2,5.3] we found an efficient way to compute these multiplicators $\beta_{\mathfrak{P}}$ in terms of the data supported by the OM representations. They are elements in $B_{\mathfrak{p}}$ of the form:

$$\beta_{\mathfrak{P}} = \pi^{-N} \prod_{\mathfrak{Q}\mid\mathfrak{p},\, \mathfrak{Q}\neq\mathfrak{P}} \phi_{\mathfrak{Q}}(\theta)^{d_{\mathfrak{Q}}}, \quad \phi_{\mathfrak{Q}} := \phi_{r_{\mathfrak{Q}}+1,\mathfrak{Q}}$$

An adequate choice of the exponents $d_{\mathfrak{Q}}$, N leads to $w_{\mathfrak{P}}(\beta_{\mathfrak{P}}) = 0$. Also, we can get $w_{\mathfrak{Q}}(\beta_{\mathfrak{P}})$ high enough by improving to an adequate precision the Okutsu approximation $\phi_{\mathfrak{Q}}$ to the factor $F_{\mathfrak{Q}}$ with the single-factor lifting algorithm [9].

Although the local bases are a by-product of the Montes algorithm, the construction of these multiplicators requires extra work. In section 4 we shall construct local bases by using *quotients* instead of ϕ-polynomials. These quotients are $\mathfrak{p}$-integral (and not only $\mathfrak{P}$-integral). In section 5 we shall use this fact to construct $\mathfrak{p}$-integral bases with no need to compute multiplicators (Theorem 5.16).

If A is a PID, then B is a free A-module of rank n. If we take $\pi \in A$ to be a generator of the principal ideal $\mathfrak{p}$, then the $\mathfrak{p}$-integral bases constructed as above are made of global integral elements because $\mathfrak{p}$ is the only prime ideal of A that divides the denominators.

If for all prime ideals $\mathfrak{p}$ dividing the discriminant of $f(x)$ we compute a $\mathfrak{p}$-integral basis in Hermite normal form, then an easy application of the CRT yields a global integral basis; that is, a basis of B as an A-module.

3. Quotients of ϕ-adic expansions

We keep all notation from the preceding section.

Let $\phi(x) \in A[x]$ be a monic polynomial of positive degree and let

$$f(x) = a_0(x) + a_1(x)\phi(x) + \cdots + a_m(x)\phi(x)^m, \quad a_s(x) \in A[x],\ \deg a_s < \deg \phi,$$

be the canonical ϕ-expansion of $f(x)$. Note that $m = \lfloor \deg f / \deg \phi \rfloor$.

Definition 3.1. *The ϕ-*quotients of $f(x)$ *are the quotients $Q_1(x), \ldots, Q_m(x)$, obtained along the computation of the coefficients of the ϕ-expansion of $f(x)$:*

$$\begin{aligned} f(x) &= \phi(x)\, Q_1(x) + a_0(x), \\ Q_1(x) &= \phi(x)\, Q_2(x) + a_1(x), \\ &\cdots \quad \cdots \\ Q_m(x) &= \phi(x) \cdot 0 + a_m(x) = a_m(x). \end{aligned}$$

Equivalently, $Q_s(x)$ is the quotient of the division of $f(x)$ by $\phi(x)^s$; we denote by $r_s(x)$ the remainder of this division. Thus, for all $1 \le i \le m$ we have,

$$f(x) = r_s(x) + Q_s(x)\phi(x)^s,\ r_s(x) = a_0(x) + a_1(x)\phi(x) + \cdots + a_{s-1}(x)\phi(x)^{s-1}. \tag{3}$$

The aim of this section is to use these quotients to construct nice $\mathfrak{p}$-integral elements. More precisely, for certain ϕ-quotients $Q(x)$ of $f(x)$, we find the highest exponent μ such that $Q(\theta)/\pi^\mu$ is $\mathfrak{p}$-integral (Theorem 3.3 and Corollary 3.7).

3.1. **Construction of integral elements.**

Lemma 3.2. *Let $\mathbf{t} = (\psi_0; \cdots; (\phi_r, \lambda_r, \psi_r))$ be a type over $\mathcal{O}_\mathfrak{p}$ of order $r \ge 1$. Fix an index $1 \le i \le r$. Let $g(x) \in A[x]$ be a polynomial of degree less than m_{r+1}, and consider its multiadic expansion:*

$$g(x) = \sum\nolimits_{\mathbf{j}=(j_i,\dots,j_r)} a_\mathbf{j}(x)\Phi(x)^\mathbf{j}, \quad \deg a_\mathbf{j} < m_i,$$

where $\Phi(x)^\mathbf{j} := \phi_i(x)^{j_i}\cdots\phi_r(x)^{j_r}$, and $0 \le j_k < e_k f_k$, for all $i \le k \le r$. Then, $v_{r+1}(g) = \min\left\{v_{r+1}(a_\mathbf{j}(x)\Phi(x)^\mathbf{j}) \mid \mathbf{j} = (j_i, \dots, j_r)\right\}$.

Proof. Since v_{r+1} is a valuation, it suffices to show that $v_{r+1}\left(a_\mathbf{j}(x)\Phi(x)^\mathbf{j}\right) \ge v_{r+1}(g)$ for all $\mathbf{j}$. Let us prove this inequality by induction on $r-i$. For $r = i$ this is proven in [7, Prop. 2.7,(4)]. Suppose that $r > i$ and the lemma is true for the indices $r-1 \ge i$. Consider the ϕ_r-expansion of $g(x)$, and the $(\phi_i, \dots, \phi_{r-1})$-multiadic development of each coefficient:

$$g(x) = \sum_{0\le j<e_rf_r} g_j(x)\phi_r(x)^j, \quad g_j(x) = \sum_{\mathbf{j}=(j_i,\dots,j_{r-1},j)} a_\mathbf{j}(x)\phi_i(x)^{j_i}\cdots\phi_{r-1}(x)^{j_{r-1}}.$$

By the definition of v_{r+1}, we have $v_{r+1}(P) = e_r v_r(P)$, for any polynomial $P \in A[x]$ of degree less than m_r. Thus, by [7, Prop. 2.7,(4)] and the induction hypothesis:

$$\begin{aligned} v_{r+1}(g) &\le v_{r+1}\left(g_j(x)\phi_r(x)^j\right) = e_r v_r(g_j) + j v_{r+1}(\phi_r) \\ &\le e_r v_r\left(a_\mathbf{j}(x)\phi_i(x)^{j_i}\cdots\phi_{r-1}(x)^{j_{r-1}}\right) + j v_{r+1}(\phi_r) = v_{r+1}\left(a_\mathbf{j}(x)\Phi(x)^\mathbf{j}\right), \end{aligned}$$

for all $0 \le j < e_r f_r$, and all $\mathbf{j} = (j_i, \dots, j_r)$ such that $j_r = j$. □

For any pair $i < r$ of positive integers, two of the formulas from [7, Prop. 2.15] can be rewritten as:

$$\frac{v_r(\phi_r)}{e_1\cdots e_{r-1}} = \sum_{1\le j<r} \frac{m_r}{m_j}\,\frac{h_j}{e_1\cdots e_j}, \quad \frac{v_r(\phi_i)}{e_1\cdots e_{r-1}} = \sum_{1\le j\le i} \frac{m_i}{m_j}\,\frac{h_j}{e_1\cdots e_j}. \tag{4}$$

Recall that $V_i := v_i(\phi_i)$. We deduce from these identities:

$$\frac{V_r}{e_1\cdots e_{r-1}} = \frac{m_r}{m_i}\,\frac{V_i}{e_0\cdots e_{i-1}} + \sum_{i\le j<r} \frac{m_r}{m_j}\,\frac{h_j}{e_1\cdots e_j}, \tag{5}$$

$$\frac{v_r(\phi_i)}{e_1\cdots e_{r-1}} = \frac{V_i}{e_0\cdots e_{i-1}} + \frac{h_i}{e_1\cdots e_i}. \tag{6}$$

Theorem 3.3. *Let $\mathbf{t} = (\psi_0; \cdots; (\phi_{r-1}, \lambda_{r-1}, \psi_{r-1}))$ be a type over $\mathcal{O}_\mathfrak{p}$ of order $r-1 \ge 0$ and let ϕ_r be a representative of $\mathbf{t}$. Suppose that $\mathbf{t} \mid f(x)$ and all polynomials $\phi_1, \dots, \phi_r$ have coefficients in A. For any integer $1 \le s \le \ell(N_r^-(f))$,*

FIGURE 1

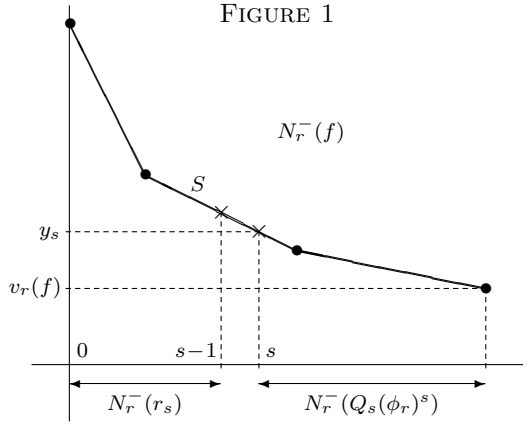
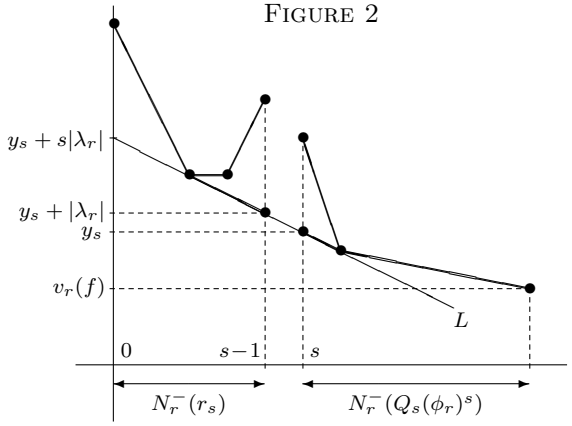


FIGURE 2



let $Q_s(x)$ be the s-th ϕ_r-quotient of $f(x)$ and let $y_s \in \mathbb{Q}$ be determined by $(s, y_s) \in N_r^-(f)$. Then, for every prime ideal $\mathfrak{P}$ of B lying over $\mathfrak{p}$, we have:

$$w_{\mathfrak{P}}(Q_s(\theta)) \geq H_s := (y_s - sV_r)/(e_0 \cdots e_{r-1}). \tag{7}$$

In particular, $Q_s(\theta)/\pi^{\lfloor H_s \rfloor}$ is $\mathfrak{p}$-integral.

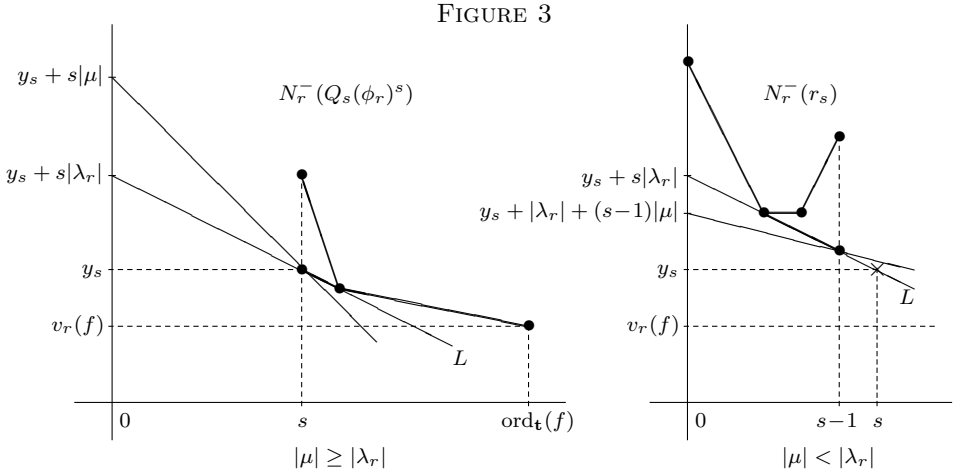
Proof. Let $\lambda_r = -h_r/e_r$, with h_r, e_r positive coprime integers, be the slope of the side S of $N_r^-(f)$, whose projection to the horizontal axis contains the abscissa s. If s is the abscissa of a vertex of $N_r^-(f)$, then we take S to be the left adjacent side.

The identities (3) show that $N_r^-(f)$ should split in principle into two parts: $N_r^-(r_s)$ and $N_r^-(Q_s(\phi_r)^s)$ (see Figure 1). This is not always true because, depending on the values of $v_r(a_{s-1}(\phi_r)^{s-1})$ and $v_r(a_s(\phi_r)^s)$, the two parts of the side S in the polygons $N_r^-(r_s)$ and $N_r^-(Q_s(\phi_r)^s)$ might change. Figure 2 shows different possibilities for these changes. However, the line L of slope λ_r that first touches both polygons from below is still the line determined by S.

A prime ideal $\mathfrak{P} \mid \mathfrak{p}$ satisfies one and only one of the following conditions:

(i) $\mathbf{t} \mid F_{\mathfrak{P}}$.
(ii) $\mathbf{t} \nmid F_{\mathfrak{P}}$, but $\mathbf{t}' \mid F_{\mathfrak{P}}$, for $\mathbf{t}' = \mathrm{Trunc}_{i-1}(\mathbf{t})$ and some maximal $1 \leq i < r$.
(iii) $\mathrm{Trunc}_0(\mathbf{t}) \nmid F_{\mathfrak{P}}$, or equivalently, $\psi_0 \nmid \overline{F}_{\mathfrak{P}}$.

FIGURE 3



We shall prove the inequality (7) by an independent argument in each case. We denote throughout the proof: $e = e_0 \cdots e_{r-1}$.

Case (i): $\mathbf{t} \mid F_{\mathfrak{P}}$

By [7, Thm. 3.1], for some slope μ of $N_r^-(f)$, we have:

$$w_{\mathfrak{P}}(\phi_r(\theta)) = (V_r + |\mu|)/e, \tag{8}$$

and $N_r(F_{\mathfrak{P}})$ is one-sided of slope μ. Consider the type $\tilde{\mathbf{t}} := (\mathbf{t}; (\phi_r, \mu, \psi))$, where ψ is the monic irreducible factor of $R_{\mu,r}(F_{\mathfrak{P}})$ [7, Thm. 3.7]. By construction, $\tilde{\mathbf{t}} \mid F_{\mathfrak{P}}$.

If $|\mu| \geq |\lambda_r|$, then Proposition 1.5 applied to the type $\tilde{\mathbf{t}}$ and the polynomial $Q_s(x)\phi_r(x)^s$ shows that (see Figure 3):

$$w_{\mathfrak{P}}(Q_s(\theta)\phi_r(\theta)^s) \geq (y_s + s|\mu|)/e.$$

By (8), we get $w_{\mathfrak{P}}(Q_s(\theta)) \geq H_s$, as desired.

If $|\mu| < |\lambda_r|$, we apply Proposition 1.5 to the type $\tilde{\mathbf{t}}$ and the polynomial $r_s(x)$ and we get (see Figure 3):

$$w_{\mathfrak{P}}(Q_s(\theta)\phi_r(\theta)^s) \overset{(3)}{=} w_{\mathfrak{P}}(r_s(\theta)) \geq (y_s + |\lambda_r| + (s-1)|\mu|)/e.$$

By (8), we get in this case a stronger inequality:

$$w_{\mathfrak{P}}(Q_s(\theta)) \geq H_s + (|\lambda_r| - |\mu|)/e.$$

Summing up, we get in Case (i):

$$w_{\mathfrak{P}}(Q_s(\theta)) \geq H_s + \max\{0, (|\lambda_r| - |\mu|)/e\}. \tag{9}$$

Case (ii): $\mathbf{t} \nmid F_{\mathfrak{P}}$, $\mathbf{t}' \mid F_{\mathfrak{P}}$, for $\mathbf{t}' = \mathbf{Trunc}_{i-1}(\mathbf{t})$ with i maximal, $1 \leq i < r$

As above, $N_i(F_{\mathfrak{P}})$ is one-sided of slope μ, one of the slopes of $N_i^-(f)$, and

$$w_{\mathfrak{P}}(\phi_i(\theta)) = (V_i + |\mu|)/(e_0 \cdots e_{i-1}). \tag{10}$$

On the other hand, the arguments in the proof of [8, Prop. 4.7] show that

$$w_{\mathfrak{P}}(\phi_j(\theta)) = \frac{m_j}{m_i} \frac{V_i + \min\{|\lambda_i|, |\mu|\}}{e_0 \cdots e_{i-1}}, \quad i < j \leq r. \tag{11}$$

Since $r_s(x) = \sum_{0\le t<s} a_t(x)\phi_r(x)^t$, there exists $0 \le t < s$ such that $w_{\mathfrak{P}}(r_s(\theta)) \ge w_{\mathfrak{P}}(a_t(\theta)\phi_r(\theta)^t)$; thus, by (3),

$$w_{\mathfrak{P}}(Q_s(\theta)) = w_{\mathfrak{P}}(r_s(\theta)) - sw_{\mathfrak{P}}(\phi_r(\theta)) \ge w_{\mathfrak{P}}(a_t(\theta)) - (s-t)w_{\mathfrak{P}}(\phi_r(\theta)). \tag{12}$$

Let us show that $w_{\mathfrak{P}}(a_t(\theta))$ is sufficiently large. Consider the multiadic expansion:

$$a_t(x) = \sum\nolimits_{\mathbf{j}\in J} b_{\mathbf{j}}(x)\Phi(x)^{\mathbf{j}}, \quad \deg b_{\mathbf{j}} < m_i, \tag{13}$$

where $\Phi(x)^{\mathbf{j}} := \phi_i(x)^{j_i}\cdots\phi_{r-1}(x)^{j_{r-1}}$ and $0 \le j_k < e_k f_k$ for all $i \le k < r$. Fix a multiindex $\mathbf{j}$ such that

$$w_{\mathfrak{P}}(a_t(\theta)) \ge w_{\mathfrak{P}}\left(b_{\mathbf{j}}(\theta)\Phi(\theta)^{\mathbf{j}}\right). \tag{14}$$

Since $\mathbf{t}' \mid F_{\mathfrak{P}}$ and $\deg b_{\mathbf{j}} < m_i$, [7, Props. 2.9,2.7,(1)] show that:

$$w_{\mathfrak{P}}(b_{\mathbf{j}}(\theta)) = v_i(b_{\mathbf{j}})/(e_0\cdots e_{i-1}) = v_r(b_{\mathbf{j}})/(e_0\cdots e_{r-1}). \tag{15}$$

Finally, by the convexity of the Newton polygon $N_r^-(f)$:

$$v_r\left(a_t(\phi_r)^t\right) \ge y_s + (s-t)|\lambda_r|. \tag{16}$$

If we gather (12), (14), (15), (16) and we use Lemma 3.2, we get:

$$\begin{aligned}
w_{\mathfrak{P}}(Q_s(\theta)) &\ge w_{\mathfrak{P}}(a_t(\theta)) - (s-t)w_{\mathfrak{P}}(\phi_r(\theta)) \\
&\ge w_{\mathfrak{P}}(b_{\mathbf{j}}(\theta)) + w_{\mathfrak{P}}(\Phi(\theta)^{\mathbf{j}}) - (s-t)w_{\mathfrak{P}}(\phi_r(\theta)) \\
&= v_r(b_{\mathbf{j}})/e + w_{\mathfrak{P}}(\Phi(\theta)^{\mathbf{j}}) - (s-t)w_{\mathfrak{P}}(\phi_r(\theta)) \\
&\ge (v_r(a_t) - v_r(\Phi^{\mathbf{j}}))/e + w_{\mathfrak{P}}(\Phi(\theta)^{\mathbf{j}}) - (s-t)w_{\mathfrak{P}}(\phi_r(\theta)) \\
&\ge (y_s + (s-t)|\lambda_r| - tV_r - v_r(\Phi^{\mathbf{j}}))/e + w_{\mathfrak{P}}(\Phi(\theta)^{\mathbf{j}}) - (s-t)w_{\mathfrak{P}}(\phi_r(\theta)).
\end{aligned}$$

If we add and substract sV_r/e to the last term, we get:

$$w_{\mathfrak{P}}(Q_s(\theta)) \ge H_s + (s-t)M + N, \tag{17}$$

where

$$M := \frac{V_r + |\lambda_r|}{e} - w_{\mathfrak{P}}(\phi_r(\theta)), \quad N := w_{\mathfrak{P}}(\Phi(\theta)^{\mathbf{j}}) - \frac{v_r(\Phi^{\mathbf{j}})}{e}.$$

Now, (5) and (11) provide a closed formula for M:

$$\begin{aligned}
M &= \frac{|\lambda_r|}{e} + \left(\sum_{i\le k<r} \frac{m_r}{m_k}\,\frac{h_k}{e_1\cdots e_k}\right) - \frac{m_r}{m_i}\,\frac{\min\{|\lambda_i|,|\mu|\}}{e_0\cdots e_{i-1}} \\
&= \left(\sum_{i\le k\le r} \frac{m_r}{m_k}\,\frac{h_k}{e_1\cdots e_k}\right) - \frac{m_r}{m_i}\,\frac{\min\{|\lambda_i|,|\mu|\}}{e_0\cdots e_{i-1}} \ge 0,
\end{aligned}$$

the last inequality because $h_i/(e_1\cdots e_i)=|\lambda_i|/(e_0\cdots e_{i-1})$. Also, (10), (6), (11) and (5) provide a closed formula for N:

$$\begin{aligned}N&=\sum\nolimits_{i\le k<r} j_k\left(w_{\mathfrak{P}}(\phi_k(\theta))-\frac{v_r(\phi_k)}{e}\right)\\&=j_i\frac{|\mu|-|\lambda_i|}{e_0\cdots e_{i-1}}+\sum_{i<k<r} j_k\left(\frac{m_k}{m_i}\,\frac{V_i+\min\{|\lambda_i|,|\mu|\}}{e_0\cdots e_{i-1}}-\frac{V_k}{e_1\cdots e_{k-1}}-\frac{h_k}{e_1\cdots e_k}\right)\\&=j_i\frac{|\mu|-|\lambda_i|}{e_0\cdots e_{i-1}}+\sum_{i<k<r} j_k\left(\frac{m_k}{m_i}\,\frac{\min\{|\lambda_i|,|\mu|\}}{e_0\cdots e_{i-1}}-\sum_{i\le j\le k}\frac{m_k}{m_j}\,\frac{h_j}{e_1\cdots e_j}\right).\end{aligned}$$

Since $M\ge 0$ and $s>t$, we deduce from (17) that $w_{\mathfrak{P}}(Q_s(\theta))\ge H_s+M+N$. Thus, we need to find lower bounds for $M+N$. Let us calculate first the sum of all terms of $M+N$ involving h_i, $|\lambda_i|=h_i/e_i$ and $|\mu|$. If $|\mu|\ge|\lambda_i|$, this partial sum is equal to $j_i(|\mu|-|\lambda_i|)/(e_0\cdots e_{i-1})\ge 0$, whereas for $|\mu|<|\lambda_i|$ we get

$$\frac{m_r}{m_i}\,\frac{|\lambda_i|-|\mu|}{e_0\cdots e_{i-1}}-\sum_{i\le k<r} j_k\frac{m_k}{m_i}\,\frac{|\lambda_i|-|\mu|}{e_0\cdots e_{i-1}}\ge\frac{|\lambda_i|-|\mu|}{e_0\cdots e_{i-1}},$$

because $(m_r/m_i)-\sum_{i\le k<r} j_k(m_k/m_i)\ge 1$, by Lemma 1.7.

Finally, the partial sum of the terms of $M+N$ involving h_j, for each $i<j\le r$, is equal to:

$$\frac{m_r}{m_j}\,\frac{h_j}{e_1\cdots e_j}-\sum_{j\le k<r} j_k\frac{m_k}{m_j}\,\frac{h_j}{e_1\cdots e_j}\ge\frac{h_j}{e_1\cdots e_j},$$

because $(m_r/m_j)-\sum_{j\le k<r} j_k(m_k/m_j)\ge 1$, by Lemma 1.7. Summing up, we have proven that

$$w_{\mathfrak{P}}(Q_s(\theta))\ge\ H_s+\max\left\{0,\frac{|\lambda_i|-|\mu|}{e_0\cdots e_{i-1}}\right\}+\sum_{i<j\le r}\frac{h_j}{e_1\cdots e_j}>H_s. \tag{18}$$

Case (iii): $\mathbf{Trunc}_0(\mathbf{t})\nmid F_{\mathfrak{P}}$, or equivalently, $\psi_0\nmid\overline{F}_{\mathfrak{P}}$.

The proof is similar to the previous case, but the arguments are now simplified because $w_{\mathfrak{P}}(\phi_j(\theta))=0$ for all $1\le j\le r$. Formula (12) now gives:

$$w_{\mathfrak{P}}(Q_s(\theta))=w_{\mathfrak{P}}(r_s(\theta))\ge w_{\mathfrak{P}}(a_t(\theta)),$$

for some $0\le t<s$. If we consider the multiadic expansion (13) for $i=1$, there exists a multiindex $\mathbf{j}=(j_1,\dots,j_{r-1})$ such that

$$w_{\mathfrak{P}}(a_t(\theta))\ge w_{\mathfrak{P}}(b_{\mathbf{j}}(\theta)\Phi(\theta)^{\mathbf{j}})=w_{\mathfrak{P}}(b_{\mathbf{j}}(\theta)).$$

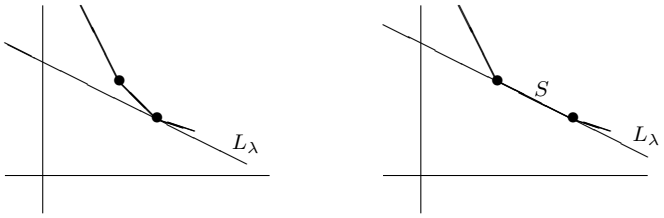
Clearly, $w_{\mathfrak{P}}(b_{\mathbf{j}}(\theta))\ge v_1(b_{\mathbf{j}})$. On the other hand, since $\deg b_{\mathbf{j}}<m_1$, the recursive definition of $v_2,\dots,v_r$ leads to $v_1(b_{\mathbf{j}})=v_r(b_{\mathbf{j}})/e$. These inequalities, together with Lemma 3.2 and (16), show that:

$$\begin{aligned}w_{\mathfrak{P}}(Q_s(\theta))\ge v_r(b_{\mathbf{j}})/e\ge\big(v_r(a_t)-v_r(\Phi^{\mathbf{j}})\big)/e\ge\big(y_s+(s-t)|\lambda_r|-tV_r-v_r(\Phi^{\mathbf{j}})\big)/e\\\ge H_s+\big((s-t)(V_r+|\lambda_r|)-v_r(\Phi^{\mathbf{j}})\big)/e\ge H_s+\big(V_r+|\lambda_r|-v_r(\Phi^{\mathbf{j}})\big)/e.\end{aligned}$$

Now, by (4):

$$\frac{V_r+|\lambda_r|-v_r(\Phi^{\mathbf{j}})}{e}=\sum_{1\le j\le r}\left(\frac{m_r}{m_j}-\sum_{j\le k<r} j_k\frac{m_k}{m_j}\right)\frac{h_j}{e_1\cdots e_j}\ge\sum_{1\le j\le r}\frac{h_j}{e_1\cdots e_j},$$

FIGURE 4. λ-component of a polygon. L_λ is the line of slope λ having first contact with the polygon from below.



the last inequality by Lemma 1.7. Thus, we obtain in this case:

$$w_{\mathfrak{P}}(Q_s(\theta)) \geq H_s + \sum\nolimits_{1\leq j\leq r} \frac{h_j}{e_1\cdots e_j} > H_s. \tag{19}$$

□

3.2. **Residual polynomials of quotients.** In this section we compute the residual polynomial $R_r(Q_s)$ of a ϕ_r-quotient of $f(x)$. To this end we recall first the general construction of the operator $R_{\lambda,i}$ of order $i>0$, with respect to a type $\mathbf{t}$ of order $i-1$, a representative ϕ_i of $\mathbf{t}$ and a negative rational number λ.

Definition 3.4. *Let $\lambda\in\mathbb{Q}_{<0}$ and N a Newton polygon. We define the* λ-component *of N to be $S_\lambda(N) := \{(x,y)\in N \mid y-\lambda x \text{ is minimal}\}$. If N has a side S of slope λ, then $S_\lambda(N)=S$; otherwise, $S_\lambda(N)$ is a vertex of N (see Figure 4).*

Let $\lambda=-h/e$, with h,e positive coprime integers. Let $g(x)=\sum_{0\leq s} a_s(x)\phi_i(x)^s$ be the canonical ϕ_i-expansion of a non-zero polynomial $g(x)\in\mathcal{O}_{\mathfrak{p}}[x]$. Let S be the λ-component of $N_i(g)$ and let s_0 be the abscissa of the left end point of S. The points of integer coordinates lying on S have abscissa $s_j := s_0+je$ for $0\leq j\leq d$, where $d:=d(S)$ is the *degree* of S.

For each $0\leq s\leq \ell(N_i^-(g))$, consider the residual coefficient $c_s\in\mathbb{F}_i$ defined as:

$$c_s := \begin{cases} 0, & \text{if } (s, v_i(a_s\phi^s)) \text{ lies above } N_i^-(g),\\ z_{i-1}^{t_{i-1}(s)} R_{i-1}(a_s)(z_{i-1}) \in \mathbb{F}_i^*, & \text{if } (s, v_i(a_s\phi^s)) \text{ lies on } N_i^-(g),\end{cases} \tag{20}$$

where $t_0(s):=0$, and $t_{i-1}(s)$ is described in [7, Def. 2.19] for $i>1$.

Definition 3.5. *The* residual polynomial *of g with respect to $(\mathbf{t},\phi_i,\lambda)$ is:*

$$R_{\lambda,i}(g)(y) := c_{s_0} + c_{s_1}y + \cdots + c_{s_d}y^d \in \mathbb{F}_i[y].$$

Since $c_{s_0}c_{s_d}\neq 0$, this polynomial has degree $d=d(S)$ and it is not divisible by y.

We now go back to the situation described in Theorem 3.3. Recall that S is the λ_r-component of $N_r^-(f)$ and $1\leq s\leq \ell(N_r^-(f))$ is an abscissa belonging to the projection of S to the horizontal axis. Denote by $d'=d(S)$ the degree of S, and let (b,u) be the right end point of S. By Definition 3.5,

$$R_r(f)(y) = c_{b-d'e_r} + c_{b-(d'-1)e_r}y + \cdots + c_b y^{d'},$$

The points of S having integer coordinates are marked in Figure 5 with $\circ$; among them, those belonging to the cloud of points $(t, v_r(a_t\phi_r^t))$ are marked with $\bullet$.

FIGURE 5

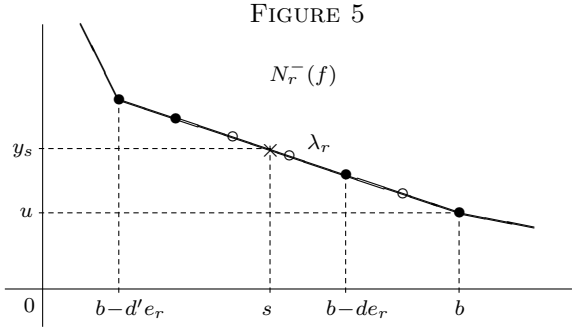
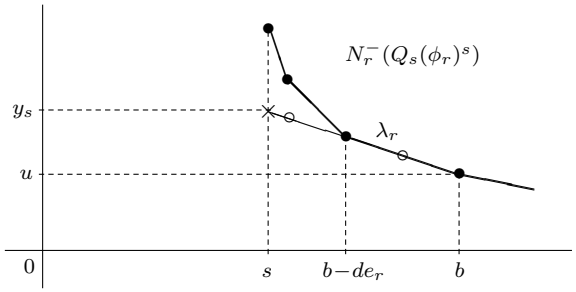


FIGURE 6



Lemma 3.6. *Let $N = N_r^-(f)$, $N' = N_r^-(Q_s(\phi_r)^s)$. Let d be the greatest integer $0 \le d \le \lfloor (b-s)/e_r \rfloor$ such that $c_{b-de_r} \neq 0$. Then, the λ_r-component of N' has left end point $(b-de_r, u+dh_r)$ and right end point (b,u). Moreover,*

$$R_r(Q_s)(y) = c_{b-de_r} + c_{b-(d-1)e_r}y + \cdots + c_b y^d.$$

Proof. By definition, $Q_s\phi_r^s = \sum_{s\le t} a_t\phi_r^t$, so that $N' := N_r^-(Q_s\phi_r^s)$ is the lower convex hull of the cloud of points $(t, v_r(a_t\phi_r^t))$, for $s \le t$ (see Figure 6). Clearly, $N' \cap ([b-de_r,\infty)\times\mathbb{R}) = N \cap ([b-de_r,\infty)\times\mathbb{R})$, and the residual coefficients of N' are $c'_t = c_t$ for all integer abscissas $s \le t \le \ell(N') = \ell(N)$. This shows that.

$$R_r(Q_s\phi_r^s)(y) = c_{b-de_r} + c_{b-(d-1)e_r}y + \cdots + c_b y^d.$$

Since $R_r(Q_s\phi_r^s) = R_r(Q_s)R_r(\phi_r)^s$ [7, Thm. 2.26] and $R_r(\phi_r) = 1$, the lemma follows. □

Corollary 3.7. *With the above notation, let $\psi_r \in \mathbb{F}_r[y]$ be a monic irreducible factor of $R_r(f)$, and consider the type $\mathbf{t}' := (\mathbf{t}; (\phi_r, \lambda_r, \psi_r))$. Let $\mathfrak{P} \mid \mathfrak{p}$ be a prime ideal of B such that $\mathbf{t}' \mid F_{\mathfrak{P}}$ and suppose $0 \le b - s < e_r f_r$. Then, $w_{\mathfrak{P}}(Q_s(\theta)) = H_s$.*

Proof. By Lemma 3.6, $\deg R_r(Q_s) \le (b-s)/e_r < f_r$; thus, $\psi_r \nmid R_r(Q_s)$. Hence, $\mathbf{t}' \nmid Q_s(x)$ and Proposition 1.5 shows that (see Figure 6)

$$w_{\mathfrak{P}}(Q_s(\theta)\phi_r(\theta)^s) = (y_s + s|\lambda_r|)/(e_0\cdots e_{r-1}).$$

On the other hand, $w_{\mathfrak{P}}(\phi_r(\theta)) = (V_r + |\lambda_r|)/(e_0\cdots e_{r-1})$, by Corollary 1.6. Therefore, $w_{\mathfrak{P}}(Q_s(\theta)) = w_{\mathfrak{P}}(Q_s(\theta)\phi_r(\theta)^s) - s w_{\mathfrak{P}}(\phi_r(\theta)) = H_s$. □

4. Quotients and local integral bases

Consider again the local context of section 1. Let k be a local field and let v, $\mathcal{O}$, $\mathfrak{m}$, π, $\mathbb{F}$ be as in that section. Also, let $F(x) \in \mathcal{O}[x]$ be a monic irreducible separable polynomial and let θ, L, $\mathcal{O}_L$, $\mathfrak{m}_L$, $\mathbb{F}_L$ be as in section 1. We indicate with a bar $\overline{\ }\colon \mathcal{O}_L \longrightarrow \mathbb{F}_L$ the reduction modulo $\mathfrak{m}_L$ homomorphism. Denote:

$$e := e(L/k), \quad f := f(L/k), \quad n_L := [L\colon k] = \deg F = ef.$$

4.1. **Local bases in standard form.** Let U_L be the group of units of $\mathcal{O}_L$ and

$$\mathbb{B} := \mathbb{B}_L := \{\alpha \in \mathcal{O}_L \mid 0 \le v(\alpha) < 1\}.$$

Lemma 4.1. *Let $\mathcal{B} \subset \mathbb{B}$ be a finite subset. Split $\mathcal{B}$ into the disjoint union:*

$$\mathcal{B} = \bigcup\nolimits_{0\le t<e} \mathcal{B}_t, \qquad \mathcal{B}_t := \{\alpha \in \mathcal{B} \mid v(\alpha) = t/e\},$$

and suppose that the following two conditions hold for all $0 \le t < e$:

(a) $\#\mathcal{B}_t = f$,

(b) *for some $\omega \in \mathcal{B}_t$, the family $\overline{\omega^{-1}\mathcal{B}_t}$ is an $\mathbb{F}$-basis of $\mathbb{F}_L$.*

Then, $\mathcal{B}$ is an $\mathcal{O}$-basis of $\mathcal{O}_L$.

Proof. Let $M \subset \mathcal{O}_L$ be the $\mathcal{O}$-module generated by the elements in $\mathcal{B}$. By condition (a), $\#\mathcal{B} = n_L$. By condition (b), $\mathcal{B} \otimes_{\mathcal{O}} \mathbb{F}$ is an $\mathbb{F}$-linearly independent family, hence an $\mathbb{F}$-basis, of $\mathcal{O}_L \otimes_{\mathcal{O}} \mathbb{F}$. Therefore, $M = \mathcal{O}_L$ by Nakayama's lemma. □

Condition (b) of the lemma does not depend of the choice of the element $\omega \in \mathcal{B}_t$. Actually, we can replace ω by any element in $\mathcal{O}_L$ having valuation t/e.

Definition 4.2. *An $\mathcal{O}$-basis $\mathcal{B}$ of $\mathcal{O}_L$ is said to be in* standard form *if $\mathcal{B} \subset \mathbb{B}$ and the two conditions of Lemma 4.1 are satisfied for all $0 \le t < e$.*

Examples.

(1) Suppose $U \subset U_L$ is a family of units such that $\overline{U}$ is an $\mathbb{F}$-basis of $\mathbb{F}_L$. Take $\omega_0, \dots, \omega_{e-1} \in \mathcal{O}_L$ such that $v(\omega_t) = t/e$ for all $0 \le t < e$. Then, $\mathcal{B} := \cup_{0\le t<e} \omega_t U$ is an $\mathcal{O}$-basis of $\mathcal{O}_L$ in standard form.

(2) The Okutsu basis $\mathcal{B} = \{g_m(\theta)/\pi^{\mu_m} \mid 0 \le m < n_L\}$ described at the end of section 1 is in standard form [16, I,Prop. 2], [7, Prop. 4.28].

Definition 4.3. *We define a* star operation *between elements of $\mathcal{O}_L \setminus \{0\}$, by:*

$$\alpha \star \beta := \alpha\beta/\pi^{\lfloor v(\alpha\beta)\rfloor} \in \mathbb{B}.$$

It is clearly associative and commutative.

Lemma 4.4. *Let $\mathcal{B}$ be an $\mathcal{O}$-basis of $\mathcal{O}_L$ in standard form. For any $\omega \in \mathcal{O}_L \setminus \{0\}$, the set $\omega \star \mathcal{B} := \{\omega \star \alpha \mid \alpha \in \mathcal{B}\}$ is an $\mathcal{O}$-basis of $\mathcal{O}_L$ in standard form.*

Proof. Let $\Pi \in \mathcal{O}_L$ be a uniformizer. Write $\omega = \Pi^m\eta$ for some unit $\eta \in U_L$ and some exponent $m \ge 0$. Clearly, $\omega \star \mathcal{B} = \Pi \star \cdots \star \Pi \star \eta \star \mathcal{B}$. Thus, it is sufficient to check that $\eta \star \mathcal{B}$ and $\Pi \star \mathcal{B}$ are bases in standard form. For $\eta \star \mathcal{B} = \eta\mathcal{B}$ this is obvious. For $\Pi \star \mathcal{B}$ we have

$$\Pi \star \mathcal{B} = \bigcup\nolimits_{0\le t<e} \mathcal{B}'_t, \quad \mathcal{B}'_t := \begin{cases} \Pi\mathcal{B}_{t-1}, & \text{if } t > 0, \\ (\Pi/\pi)\mathcal{B}_{e-1}, & \text{if } t = 0. \end{cases}$$

Clearly, the sets $\mathcal{B}'_t$ satisfy the conditions of Lemma 4.1 for all $0 \le t < e$. □

4.2. **Quotients and local bases.** Let $\mathbf{t} = (\psi_0; (\phi_1, \lambda_1, \psi_1); \cdots, (\phi_r, \lambda_r, \psi_r))$ be an F-complete type of order r. By [7, Cor. 3.8] we have $e = e_0e_1 \cdots e_r$, $f = f_0f_1 \cdots f_r$.

To this type $\mathbf{t}$ we may attach several rational functions in $k(x)$ [7, Sec. 2.4]. Let $\pi_0(x) = 1$, $\pi_1(x) = \pi$. We define recursively for all $1 \leq i \leq r$,

$$\Phi_i(x) = \frac{\phi_i(x)}{\pi_{i-1}(x)^{V_i/e_{i-1}}}, \qquad \gamma_i(x) = \frac{\Phi_i(x)^{e_i}}{\pi_i(x)^{h_i}}, \qquad \pi_{i+1}(x) = \frac{\Phi_i(x)^{\ell_i}}{\pi_i(x)^{\ell_i'}}. \tag{21}$$

These rational functions can be written as a product of powers of $\pi, \phi_1(x), \ldots, \phi_r(x)$, with integer exponents. Recall that ℓ_i, ℓ_i' are integers satisfying the identity $\ell_i h_i - \ell_i' e_i = 1$ (section 1).

The type $\mathbf{t}$ determines as well a chain of extensions of the residue field of k:

$$\mathbb{F} = \mathbb{F}_0 \subset \mathbb{F}_1 \subset \cdots \subset \mathbb{F}_{r+1}, \qquad \mathbb{F}_{i+1} = \mathbb{F}[z_0, \ldots, z_i],\ 0 \leq i \leq r.$$

The residue field $\mathbb{F}_L$ can be identified with $\mathbb{F}_{r+1}$. More precisely, in [7, (27)] we construct an explicit isomorphism

$$\gamma\colon \mathbb{F}_{r+1} \longrightarrow \mathbb{F}_L, \qquad z_0 \mapsto \overline{\theta},\ z_1 \mapsto \overline{\gamma_1(\theta)},\ \ldots,\ z_r \mapsto \overline{\gamma_r(\theta)}, \tag{22}$$

where $\gamma_i(x) \in k(x)$ are the rational functions defined in (21).

We denote by $\mathrm{red}_L\colon \mathcal{O}_L \longrightarrow \mathbb{F}_{r+1}$ the reduction map obtained by composition of the canonical reduction map with the inverse of this isomorphism:

$$\mathrm{red}_L\colon \mathcal{O}_L \longrightarrow \mathbb{F}_L \xrightarrow{\gamma^{-1}} \mathbb{F}_{r+1}.$$

The following proposition is easily deduced from [7, Prop. 3.5].

Proposition 4.5. *Let F, θ, L, $\mathbf{t}$ be as above. Let $g(x) \in \mathcal{O}[x]$ be a non-zero polynomial and let (s, u) be the left end point of the λ_r-component of $N_r(g)$ (Definition 3.4). If $\mathbf{t} \nmid g$, then $v(g(\theta)) = v(\Phi_r(\theta)^s \pi_r(\theta)^u)$ and*

$$\mathrm{red}_L\left(g(\theta)/(\Phi_r(\theta)^s \pi_r(\theta)^u)\right) = R_r(g)(z_r) \neq 0.$$

Notation 4.6. *Let $f(x) \in \mathcal{O}[x]$ be a monic separable polynomial, divisible by $F(x)$ in $\mathcal{O}[x]$. For all $1 \leq i \leq r$, we denote*

(b_i, u_i)	*the right end point of the side of slope λ_i of $N_i^-(f)$*
u_i'	$= u_i - b_iV_i$
$Q_{i,j}(x)$	*the $(b_i - j)$-th ϕ_i-quotient of $f(x)$, for $0 \leq j < b_i$*
$y_{i,j}$	*the ordinate of the point of $N_i^-(f)$ with abscissa $b_i - j$*
$H_{i,j}$	$= (y_{i,j} - (b_i - j)V_i)/(e_0 \cdots e_{i-1}) = (u_i' + j(V_i + \lvert\lambda_i\rvert))/(e_0 \cdots e_{i-1})$

We emphasize that j is the distance from the relevant abscissa $b_i - j$ of the quotient to the abscissa b_i of the right end point of the relevant side of $N_i^-(f)$. Figure 7 illustrates the situation.

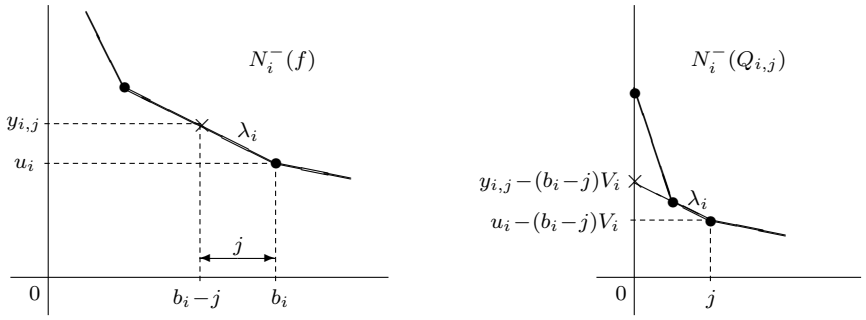
The aim of this section is to prove the following result.

Theorem 4.7. *Let $J = \{(j_0, \ldots, j_r) \in \mathbb{N}^{r+1} \mid 0 \leq j_i < e_if_i,\ \forall\, 0 \leq i \leq r\}$ and for each multiindex $\mathbf{j} \in J$, consider:*

$$Q_{\mathbf{j}} := \theta^{j_0} Q_{1,j_1}(\theta) \star \cdots \star Q_{r,j_r}(\theta) = \frac{\theta^{j_0} Q_{1,j_1}(\theta) \cdots Q_{r,j_r}(\theta)}{\pi^{\lfloor H_{1,j_1} + \cdots + H_{r,j_r} \rfloor}} \in \mathbb{B}.$$

Then, the family $\mathcal{B} := \{Q_{\mathbf{j}} \mid \mathbf{j} \in J\}$ is an $\mathcal{O}$-basis of $\mathcal{O}_L$ in standard form.

FIGURE 7



By (1), $v(\theta^{j_0}) = 0$ because $0 \le j_0 < e_0 f_0 = m_1$. Also, $v(Q_{i,j_i}(\theta)) = H_{i,j_i}$ for all i, by Corollary 3.7. Thus, $Q_{\mathbf{j}}$ indeed belongs to $\mathbb{B}$. In order to prove Theorem 4.7 we need to check that the sets $\mathcal{B}_t = \{\alpha \in \mathcal{B} \mid v(\alpha) = t/e\}$ satisfy the conditions of Lemma 4.1. This will be shown by a recursive argument.

Consider the filtration of $\mathbb{B}$ determined by the subsets:

$$U_L = \mathbb{B}_0 \subset \mathbb{B}_1 \subset \cdots \subset \mathbb{B}_r = \mathbb{B}, \quad \mathbb{B}_i := \{\alpha \in \mathbb{B} \mid e_0 \cdots e_i \, v(\alpha) \in \mathbb{Z}\}.$$

For $0 \le i \le r$, $\mathbb{B}_i$ splits as the disjoint union:

$$\mathbb{B}_i = \bigcup\nolimits_{0 \le t < e_0 \cdots e_i} \mathbb{B}_{i,t}, \qquad \mathbb{B}_{i,t} := \{\alpha \in \mathbb{B}_i \mid v(\alpha) = t/e_0 \cdots e_i\}.$$

Definition 4.8. *We say that $B \subset \mathbb{B}_i$ is a* level i basis in standard form *if for all $0 \le t < e_0 \cdots e_i$, the following two conditions are satisfied:*

(1) *$\#B_t = f_0 \cdots f_i$, where $B_t := B \cap \mathbb{B}_{i,t}$,*
(2) *For any $\omega \in \mathbb{B}_{i,t}$, the family $\mathrm{red}_L(\omega^{-1} B_t)$ is an $\mathbb{F}$-basis of $\mathbb{F}_{i+1}$.*

Lemma 4.9. *Let $B \subset \mathbb{B}_{i-1}$ be a level $i-1$ basis in standard form, for some $1 \le i \le r$. For each $0 \le t < e_0 \cdots e_i$, take $0 \le q_t < e_i$ such that $q_t h_i \equiv t \pmod{e_i}$.*

(a) Let $\{\omega_j\}_{0 \le j < e_i f_i} \subset \mathbb{B}_i$ such that $e_0 \cdots e_i \, v(\omega_j) \equiv j h_i \pmod{e_i}$ for all j. Then,

(i) *If $j \not\equiv q_t \pmod{e_i}$, then $(\omega_j \star B) \cap \mathbb{B}_{i,t} = \emptyset$.*
(ii) *For each $j = q_t + k e_i$, there exists a unique $0 \le t_k < e_0 \cdots e_{i-1}$, depending on i, t, k and $v(\omega_j)$, such that $\omega_j \star B_{t_k} \subset \mathbb{B}_{i,t}$.*

(b) Suppose moreover that for some $\Pi \in \mathbb{B}_{i,1}$, $\Pi_0 \in \mathbb{B}_{i-1,1}$, the family

$$\epsilon_k := \mathrm{red}_L\left(\Pi^{-t} \omega_{q_t + k e_i} \star (\Pi_0)^{t_k}\right), \quad 0 \le k < f_i,$$

is an $\mathbb{F}_i$-basis of $\mathbb{F}_{i+1}$ for all $0 \le t < e_0 \cdots e_i$. Then, $B' := \bigcup_{0 \le j < e_i f_i} \omega_j \star B \subset \mathbb{B}_i$ is a level i basis in standard form.

Proof. Let $e_0 \cdots e_i \, v(\omega_j) = j h_i + p_j e_i$ for some integer p_j. For $0 \le t' < e_0 \cdots e_{i-1}$, the condition $\omega_j \star B_{t'} \subset \mathbb{B}_{i,t}$ is equivalent to:

$$v(\omega_j) + t'/(e_0 \cdots e_{i-1}) \equiv t/(e_0 \cdots e_i) \pmod{\mathbb{Z}},$$

or, equivalently,

$$j h_i + p_j e_i + t' e_i \equiv t \pmod{e_0 \cdots e_i}. \tag{23}$$

The condition $jh_i \equiv t \pmod{e_i}$, or equivalently, $j \equiv q_t \pmod{e_i}$, is necessary. On the other hand, if we denote $n_{i,t} := (q_t h_i - t)/e_i$, and we take $j = q_t + ke_i$, then there is a unique $0 \le t' < e_0 \cdots e_{i-1}$ for which (23) holds:

$$t' \equiv -(n_{i,t} + kh_i + p_j) \pmod{e_0 \cdots e_{i-1}}.$$

This proves items (i) and (ii) of the lemma. Therefore, the set B' splits as:

$$B' = \bigcup\nolimits_{0 \le t < e_0 \cdots e_i} B'_t, \qquad B'_t = \bigcup\nolimits_{0 \le k < f_i} \omega_{q_t + ke_i} \star B_{t_k}.$$

In particular, $\#B'_t = f_i \# B_{t_k} = f_0 \cdots f_i$.

Finally, by the hypothesis on B, for any given t as above the sets B_{t_k} can be expressed as $B_{t_k} = (\Pi_0)^{t_k} U_k$, for a set $U_k \subset U_L$ such that $\mathrm{red}_L(U_k)$ is an $\mathbb{F}$-basis of $\mathbb{F}_i$. Hence, if the family $(\epsilon_k)_{0 \le k < f_i}$ is an $\mathbb{F}_i$-basis of $\mathbb{F}_{i+1}$, then the family

$$\mathrm{red}_L(\Pi^{-t} B'_t) = \bigcup\nolimits_{0 \le k < f_i} \epsilon_k \, \mathrm{red}_L(U_k)$$

is an $\mathbb{F}$-basis of $\mathbb{F}_{i+1}$. □

Lemma 4.9 can be applied to construct different local integral bases in standard form. Starting with $B_0 = \{1, \theta, \cdots, \theta^{f_0 - 1}\}$, we recursively construct, for $1 \le i \le r$,

$$B_i = \bigcup\nolimits_{0 \le j < e_i f_i} \omega_{i,j} \star B_{i-1},$$

with $\omega_{i,j}$ satisfying the conditions of Lemma 4.9. For instance, we can take $\omega_{i,j} = \phi_i(\theta)^j$ and we reobtain Okutsu's basis described in Theorem 1.8.

Let us apply this idea to the quotients. For all $0 \le i \le r$, consider the set

$$B_i := \{\theta^{j_0} Q_{1,j_1}(\theta) \star \cdots \star Q_{i,j_i}(\theta) \mid 0 \le j_k < e_k f_k, \ \forall\, 0 \le k \le i\} \subset \mathbb{B}_i.$$

Since $\mathcal{B} = B_r$ and $\mathbb{F}_{r+1} \simeq \mathbb{F}_L$, Theorem 4.7 is a consequence of the following result.

Proposition 4.10. *For all $0 \le i \le r$, the set B_i is a level i basis in standard form.*

Proof. We prove the proposition by induction on i. For $i = 0$, we have $B_0 = \{1, \theta, \ldots, \theta^{f_0 - 1}\}$ and the statement is clear. Suppose $i > 0$ and B_{i-1} is a level $i-1$ basis in standard form. In order to show that B_i is a level i basis in standard form we need only to check that the family $\omega_j := Q_{i,j}(\theta)$, for $0 \le j < e_i f_i$, satisfies the conditions (a) and (b) of Lemma 4.9.

By an equality in Notation 4.6, condition (a) on $v(\omega_j)$ is clearly satisfied:

$$e_0 \cdots e_i \, v(\omega_j) = e_0 \cdots e_i \, H_{i,j} = u'_i e_i + j(e_i V_i + h_i) \equiv jh_i \pmod{e_i}.$$

Let us prove condition (b). The rational functions $\pi_i(x)$, $\pi_{i+1}(x)$ defined in (21) satisfy [7, Cor. 3.2]:

$$v(\pi_i(\theta)) = 1/(e_0 \cdots e_{i-1}), \quad v(\pi_{i+1}(\theta)) = 1/(e_0 \cdots e_i).$$

By taking $\Pi := \pi_{i+1}(\theta)$, $\Pi_0 := \pi_i(\theta)$, we need only to show that, for any $0 \le t < e_0 \cdots e_i$, the family $(\epsilon_k)_{0 \le k < f_i}$ considered in (b) is an $\mathbb{F}_i$-basis of $\mathbb{F}_{i+1}$.

Let $0 \le t < e_0 \cdots e_i$ and consider the integer $0 \le q_t < e_i$ of Lemma 4.9. Since $\ell_i h_i - \ell'_i e_i = 1$, the integer $N := (q_t - \ell_i t)/e_i$ depends only on i and t. Clearly, $(q_t h_i - t)/e_i = Nh_i + \ell'_i t$.

We fix an integer $0 \le k < f_i$ and we let $j := q_t + ke_i$. By (a) of Lemma 4.9, there is a unique $0 \le t_k < e_0 \cdots e_{i-1}$ such that

$$n_k := H_{i,j} + t_k/(e_0 \cdots e_{i-1}) - t/(e_0 \cdots e_i)$$

is a non-negative integer that depends on i, t and k. We can express:

$$\begin{aligned} e_0\cdots e_{i-1}n_k &= u_i' + j(V_i + |\lambda_i|) + t_k - t/e_i \\ &= u_i' + jV_i + kh_i + t_k + (q_t h_i - t)/e_i \\ &= u_i' + jV_i + kh_i + t_k + Nh_i + \ell_i' t. \end{aligned} \tag{24}$$

By definition, $\epsilon_k \in \mathbb{F}_{i+1}$ is the image under red_L of the unit

$$\pi_{i+1}(\theta)^{-t} Q_{i,j}(\theta) \star \pi_i(\theta)^{t_k} = \frac{Q_{i,j}(\theta)\pi_i(\theta)^{t_k}}{\pi^{n_k}\pi_{i+1}(\theta)^t}. \tag{25}$$

Figure 6 shows the shape of $N_i^-(Q_{i,j}(\phi_i)^{b_i-j})$. Let d_k be the degree of $R_i(Q_{i,j})$. By Lemma 3.6, $d_k \le \lfloor j/e_i \rfloor = k < f_i$, and the left end point of the λ_i-component of this polygon is $(b_i - d_k e_i, u_i + d_k h_i)$. Clearly, the Newton polygon $N_i^-(Q_{i,j})$ is the image of the former polygon under the following transformation of the plane:

$$(x, y) \mapsto (x - (b_i - j), y - (b_i - j)V_i).$$

Hence, $R_i(Q_{i,j})(y)$ is not divisible by $\psi_i(y)$ and the left end point of the λ_i-component of $N_i^-(Q_{i,j})$ has coordinates $(j - d_k e_i, u_i' + jV_i + d_k h_i)$. By Proposition 4.5,

$$\mathrm{red}_L\left(\frac{Q_{i,j}(\theta)}{\Phi_i(\theta)^s \pi_i(\theta)^u}\right) = R_i(Q_{i,j})(z_i) \in \mathbb{F}_{i+1}^*, \tag{26}$$

where $s = j - d_k e_i$ and $u = u_i' + jV_i + d_k h_i$.

We can express the unit (25) as the product of two units:

$$\frac{Q_{i,j}(\theta)\pi_i(\theta)^{t_k}}{\pi^{n_k}\pi_{i+1}(\theta)^t} = \frac{Q_{i,j}(\theta)}{\Phi_i(\theta)^s\pi_i(\theta)^u} \cdot \frac{\Phi_i(\theta)^s \pi_i(\theta)^{u+t_k}}{\pi^{n_k}\pi_{i+1}(\theta)^t}, \tag{27}$$

and the residue class of the first factor is computed in (26). If we use the following identities from (21):

$$\pi_{i+1}(\theta) = \Phi_i(\theta)^{\ell_i}/\pi_i(\theta)^{\ell_i'}, \quad \gamma_i(\theta) = \Phi_i(\theta)^{e_i}/\pi_i(\theta)^{h_i},$$

and the identity (24), the second unit may be simplified into:

$$\begin{aligned} \frac{\Phi_i(\theta)^s\pi_i(\theta)^{u+t_k}}{\pi^{n_k}\pi_{i+1}(\theta)^t} &= \pi^{-n_k}\Phi_i(\theta)^{j-d_k e_i - \ell_i t}\pi_i(\theta)^{u_i' + jV_i + d_k h_i + t_k + \ell_i' t} \\ &= \pi^{-n_k}\Phi_i(\theta)^{e_i(N+k-d_k)}\pi_i(\theta)^{e_0\cdots e_{i-1}n_k - h_i(N+k-d_k)} \\ &= \pi^{-n_k}\pi_i(\theta)^{e_0\cdots e_{i-1}n_k}\gamma_i(\theta)^{N+k-d_k}. \end{aligned}$$

By (22), the reduction of the gamma factor is immediate:

$$\mathrm{red}_L(\gamma_i(\theta)^{N+k-d_k}) = z_i^{N+k-d_k}.$$

The unit $\pi^{-1}\pi_i(\theta)^{e_0\cdots e_{i-1}}$ depends only on i; hence,

$$\tau_k := \mathrm{red}_L(\pi^{-n_k}\pi_i(\theta)^{e_0\cdots e_{i-1}n_k}) = \mathrm{red}_L(\pi^{-1}\pi_i(\theta)^{e_0\cdots e_{i-1}})^{n_k}$$

is a non-zero element in $\mathbb{F}_i$ that depends on i, t and k.

From (25), (26), (27) and Lemma 3.6 we get:

$$\begin{aligned} \epsilon_k &= \mathrm{red}_L\left(\frac{Q_{i,j}(\theta)\pi_i(\theta)^{t_k}}{\pi^{n_k}\pi_{i+1}(\theta)^t}\right) = R_i(Q_{i,j})(z_i)\cdot\tau_k\cdot z_i^{N+k-d_k} \\ &= \tau_k \cdot z_i^N\left(c_{b_i-d_k e_i} z_i^{k-d_k} + c_{b_i-(d_k-1)e_i} z_i^{k-d_k+1} + \cdots + c_{b_i} z_i^k\right). \end{aligned} \tag{28}$$

Since c_{b_i} is always non-zero, and N does not depend on k, the family of all ϵ_k, for $0 \le k < f_i$, is an $\mathbb{F}_i$-basis of $\mathbb{F}_{i+1}$. □

4.3. **A variation on Theorem 4.7.** We can simplify a little bit some quotients and still get an integral basis. For all $1 \le i \le r$, $0 \le j < b_i$, define

$$Q'_{i,j}(x) := \begin{cases} Q_{i,j}(x), & \text{if } j \neq 0, \\ 1, & \text{if } j = 0, \end{cases} \qquad H'_{i,j} := \begin{cases} H_{i,j}, & \text{if } j \neq 0, \\ 0, & \text{if } j = 0, \end{cases} \tag{29}$$

where $Q_{i,j}$, $H_{i,j}$ have still the meaning of Notation 4.6.

Theorem 4.11. *Let $J = \{(j_0, \dots, j_r) \in \mathbb{N}^{r+1} \mid 0 \le j_i < e_i f_i,\ \forall\, 0 \le i \le r\}$, and for each multiindex $\mathbf{j} \in J$ denote:*

$$Q'_{\mathbf{j}} := \theta^{j_0} Q'_{1,j_1}(\theta) \star \cdots \star Q'_{r,j_r}(\theta) = \frac{\theta^{j_0} Q'_{1,j_1}(\theta) \cdots Q'_{r,j_r}(\theta)}{\pi^{\lfloor H'_{1,j_1} + \cdots + H'_{r,j_r} \rfloor}} \in \mathbb{B}.$$

Then the family $\mathcal{B}' := \{Q'_{\mathbf{j}} \mid \mathbf{j} \in J\}$ is an $\mathcal{O}$-basis of $\mathcal{O}_L$ in standard form.

Proof. For each $0 \le i \le r$, consider the following set:

$$B'_i := \{\theta^{j_0} Q'_{1,j_1}(\theta) \star \cdots \star Q'_{i,j_i}(\theta) \mid 0 \le j_k < e_k f_k,\ \forall\, 0 \le k \le i\} \subset \mathbb{B}_i.$$

Denote $\omega_j := Q_{i,j}(\theta)$, $\omega'_j := Q'_{i,j}(\theta)$ for all $0 \le j < e_i f_i$. Arguing as in the proof of Proposition 4.10, the theorem will be proven if we show that the family of all ω'_j satisfies the conditions (a) and (b) of Lemma 4.9.

Condition (a) is obvious; let us prove condition (b). For fixed $0 \le i \le r$, $0 \le t < e_0 \cdots e_i$, let $0 \le q_t < e_i$ be the integer of Lemma 4.9 and consider

$$\begin{aligned} \epsilon_k &:= \mathrm{red}_L\left(\pi_{i+1}(\theta)^{-t} \omega_{q_t + k e_i} \star \pi_i(\theta)^{t_k}\right), \qquad 0 \le k < f_i, \\ \epsilon'_k &:= \mathrm{red}_L\left(\pi_{i+1}(\theta)^{-t} \omega'_{q_t + k e_i} \star \pi_i(\theta)^{t'_k}\right), \qquad 0 \le k < f_i. \end{aligned}$$

If $q_t \neq 0$, we have $t'_k = t_k$ and $\epsilon'_k = \epsilon_k$, for all k, and we saw along the proof of Proposition 4.10 that they form an $\mathbb{F}_i$-basis of $\mathbb{F}_{i+1}$.

Suppose $q_t = 0$. Then, again, $\epsilon'_k = \epsilon_k$, for all $k \neq 0$. For $k = 0$ (i.e. $j = 0$), let us compute and compare ϵ_0 and ϵ'_0. The degree d_k of $R_i(Q_{i,0})(y)$ is zero, because $0 \le d_k \le k$; hence, (28) shows that $\epsilon_0 = \zeta z_i^N$, for some $\zeta \in \mathbb{F}_i^*$. Since $q_t = 0$, t is divisible by e_i and $N = -\ell_i t / e_i$; also, since $v(\omega'_j) = 0$, we have $t'_0 = t/e_i$. By using again (21) and $\ell_i h_i - \ell'_i e_i = 1$, we get:

$$\pi_{i+1}(\theta)^{-e_i t'_0} \pi_i(\theta)^{t'_0} = \Phi_i(\theta)^{-\ell_i e_i t'_0} \pi_i(\theta)^{t'_0 + \ell'_i e_i t'_0} = \gamma_i(\theta)^{-\ell_i t'_0} = \gamma_i(\theta)^N.$$

Hence, $\epsilon'_0 = \mathrm{red}_L(\pi_{i+1}(\theta)^{-e_i t'_0} \pi_i(\theta)^{t'_0}) = \mathrm{red}_L(\gamma_i(\theta)^N) = z_i^N$.

Thus, the family $(\epsilon'_k)_{0 \le k < f_i}$ differs from the family $(\epsilon_k)_{0 \le k < f_i}$ only in one term: $\epsilon_0 = \zeta \epsilon'_0$, for some $\zeta \in \mathbb{F}_i^*$. Since the family $(\epsilon_k)_{0 \le k < f_i}$ is an $\mathbb{F}_i$-basis of $\mathbb{F}_{i+1}$, the family $(\epsilon'_k)_{0 \le k < f_i}$ has the same property. □

5. Quotients and global $\mathfrak{p}$-integral bases

We go back to the global context of sections 2, 3, and we keep the notation from those sections. We denote by $\mathcal{P}$ the set of prime ideals of B lying above $\mathfrak{p}$.

5.1. **Reduced families of algebraic elements.** For any prime ideal $\mathfrak{P} \in \mathcal{P}$, we use a special notation for two objects attached to the OM representation $\mathbf{t}_{\mathfrak{P}}$:

$$\mathbb{F}_{\mathfrak{P}} := \mathbb{F}_{r_{\mathfrak{P}}+1, \mathfrak{P}}, \qquad \Pi_{\mathfrak{P}} := \pi_{r_{\mathfrak{P}}+1, \mathfrak{P}}(\theta) \in L^*.$$

Thus, $\mathbb{F}_{\mathfrak{P}}$ is a computational representation of the local residue field $\mathcal{O}_{\mathfrak{P}}/\mathfrak{P}\mathcal{O}_{\mathfrak{P}}$. The rational fractions $\pi_{i,\mathfrak{P}}$ were defined in (21); recall that $w_{\mathfrak{P}}(\Pi_{\mathfrak{P}}) = 1/e(\mathfrak{P}/\mathfrak{p})$.

The concept of a $\mathfrak{p}$-*reduced family* of elements of the function field of a curve was introduced by W. M. Schmidt in the context of Puiseux expansions [20, 22]. In this section we use these ideas conveniently adapted to our more general setting.

Definition 5.1. *Consider the following* $\mathfrak{p}$*-valuation mapping:*

$$w := w_{\mathfrak{p}} \colon L \longrightarrow \mathbb{Q} \cup \{\infty\}, \quad w(\alpha) = \min_{\mathfrak{P}\in\mathcal{P}}\{w_{\mathfrak{P}}(\alpha)\}.$$

Clearly, $w(a) = v_{\mathfrak{p}}(a)$ for all $a \in K$. The map w does not behave well with respect to multiplication, but it has some of the typical properties of a valuation.

Lemma 5.2. *Let* $a \in K$*, and* $\alpha, \beta \in L$*.*

(1) $w(a\alpha) = w(a) + w(\alpha) = v_{\mathfrak{p}}(a) + w(\alpha)$.
(2) $w(\alpha+\beta) \geq \min\{w(\alpha), w(\beta)\}$*, and if* $w(\alpha) \neq w(\beta)$*, then equality holds.*

Definition 5.3. *For any value* $\delta \in w(L)$*, we denote*

$$L_\delta := \{\alpha \in L \mid w(\alpha) \geq \delta\} \supset L_\delta^+ := \{\alpha \in L \mid w(\alpha) > \delta\}.$$

Note that $L_\delta \subset B_{\mathfrak{p}}$ if $\delta \geq 0$. These subgroups L_δ, L_δ^+ have a natural structure of $A_{\mathfrak{p}}$-modules. Since $\mathfrak{p}L_\delta \subset L_\delta^+$, the quotient L_δ/L_δ^+ has a natural structure of $\mathbb{F}_{\mathfrak{p}}$-vector space.

Definition 5.4. *Consider the* $\mathbb{F}_{\mathfrak{p}}$*-vector space,* $V := \prod_{\mathfrak{P}\in\mathcal{P}} \mathbb{F}_{\mathfrak{P}}$*, of dimension* $\sum_{\mathfrak{P}\in\mathcal{P}} f(\mathfrak{P}/\mathfrak{p})$*. For each* $\delta \in w(L)$*,* $\delta \geq 0$*, we define a kind of reduction map:*

$$\mathrm{red}_\delta \colon L_\delta \longrightarrow V, \quad \mathrm{red}_\delta(\alpha) = (\alpha_{\delta,\mathfrak{P}})_{\mathfrak{P}\in\mathcal{P}}, \quad \alpha_{\delta,\mathfrak{P}} = \mathrm{red}_{L_{\mathfrak{P}}}\left(i_{\mathfrak{P}}\left(\alpha\Pi_{\mathfrak{P}}^{-\lfloor e(\mathfrak{P}/\mathfrak{p})\delta\rfloor}\right)\right).$$

Note that $\alpha_{\delta,\mathfrak{P}} = 0$ if and only if $w_{\mathfrak{P}}(\alpha) > \delta$. Clearly, red_δ is an homomorphism of $A_{\mathfrak{p}}$-modules and $\ker(\mathrm{red}_\delta) = L_\delta^+$. Therefore, red_δ induces an embedding of L_δ/L_δ^+ as an $\mathbb{F}_{\mathfrak{p}}$-subspace of V.

Definition 5.5. *A finite subset* $\mathcal{B} = \{\alpha_1, \ldots, \alpha_m\} \subset L$ *is called* $\mathfrak{p}$-reduced *if for all families* $a_1, \ldots, a_m \in A_{\mathfrak{p}}$*, one has:*

$$w\left(\sum\nolimits_{1\leq i\leq m} a_i\alpha_i\right) = \min\{w(a_i\alpha_i) \mid 1 \leq i \leq m\}. \tag{30}$$

Let $\nu := \min_{1\leq i\leq m}\{v_{\mathfrak{p}}(a_i)\}$. The left and right terms of (30) diminish both by ν if we replace all a_i by $a_i' = a_i/\pi^\nu$. Thus, in order to check the equality (30) we can always assume that not all elements $a_1, \ldots, a_m \in A_{\mathfrak{p}}$ belong to $\mathfrak{p}A_{\mathfrak{p}}$.

Reduceness is a sufficient condition to ensure that certain families of elements in $B_{\mathfrak{p}}$ are a $\mathfrak{p}$-integral basis.

Lemma 5.6. *For* $n = [L\colon K]$*, let* $\mathcal{B} = \{\alpha_1, \ldots, \alpha_n\} \subset L$ *be a* $\mathfrak{p}$*-reduced set such that* $0 \leq w(\alpha) < 1$*, for all* $\alpha \in \mathcal{B}$*. Then,* $\mathcal{B}$ *is a* $\mathfrak{p}$*-integral basis of* B/A*.*

Proof. We need only to check that the elements of $\mathcal{B}$ are linearly independent modulo $\mathfrak{p}B_{\mathfrak{p}}$. Suppose $\sum_{1\leq i\leq n} a_i\alpha_i \in \mathfrak{p}B_{\mathfrak{p}}$, for certain $a_1, \ldots, a_n \in A_{\mathfrak{p}}$. Since $w\left(\sum_{1\leq i\leq n} a_i\alpha_i\right) \geq 1$ and $\mathcal{B}$ is reduced, we have $w(a_i\alpha_i) \geq 1$, for all $1 \leq i \leq n$. Since $w(\alpha_i) < 1$, this implies that $w(a_i) > 0$, or equivalently, $a_i \in \mathfrak{p}A_{\mathfrak{p}}$, for all i. □

Let us give a more practical criterion to check that a subset of L is reduced.

Lemma 5.7 (Schörnig [22])**.** *Let* $\mathcal{B} \subset L$ *be a finite subset with* $0 \leq w(\alpha) < 1$ *for all* $\alpha \in \mathcal{B}$*. For each* $\delta \in w(L)$*, denote* $\mathcal{B}_\delta = \{\alpha \in \mathcal{B} \mid w(\alpha) = \delta\}$*. Then,* $\mathcal{B}$ *is* $\mathfrak{p}$*-reduced if and only if* $\mathrm{red}_\delta(\mathcal{B}_\delta)$ *is an* $\mathbb{F}_{\mathfrak{p}}$*-linearly independent family of* V *for all* $\delta \in w(\mathcal{B})$*.*

Proof. Write $\mathcal{B} = \{\alpha_1, \dots, \alpha_m\}$ and let $I_\delta := \{1 \le i \le m \mid \alpha_i \in \mathcal{B}_\delta\}$ for each $\delta \in w(\mathcal{B})$. For any family $(a_i)_{i\in I_\delta}$ of elements in $A_\mathfrak{p}$, we clearly have:

$$\operatorname{red}_\delta\left(\sum\nolimits_{i\in I_\delta} a_i\alpha_i\right) = \sum\nolimits_{i\in I_\delta} \operatorname{red}_\delta(a_i\alpha_i) = \sum\nolimits_{i\in I_\delta} \overline{a_i}\operatorname{red}_\delta(\alpha_i), \tag{31}$$

where $\overline{a_i} \in \mathbb{F}_\mathfrak{p}$ is the class of a_i modulo $\mathfrak{p}A_\mathfrak{p}$.

Suppose $\mathcal{B}$ is a reduced set. If $\overline{a_{i_0}} \neq 0$ for some $i_0 \in I_\delta$, then $w(a_{i_0}\alpha_{i_0}) = \delta = \min_{i\in I_\delta}\{w(a_i\alpha_i)\} = w\left(\sum_{i\in I_\delta} a_i\alpha_i\right)$ and (31) shows that $\sum_{i\in I_\delta}\overline{a_i}\operatorname{red}_\delta(\alpha_i) \neq 0$. Thus, the family $\operatorname{red}_\delta(\mathcal{B}_\delta)$ is $\mathbb{F}_\mathfrak{p}$-linearly independent.

Conversely, suppose that $\operatorname{red}_\delta(\mathcal{B}_\delta)$ is an $\mathbb{F}_\mathfrak{p}$-linearly independent family of V for all $\delta \in w(\mathcal{B})$. Take $a_1, \dots, a_m \in A_\mathfrak{p}$ not all of them belonging to $\mathfrak{p}A_\mathfrak{p}$, and let

$$\delta := \min\{w(a_i\alpha_i) \mid 1 \le i \le m\}, \quad J_\delta := \{1 \le i \le m \mid w(a_i\alpha_i) = \delta\}.$$

Since $0 \le w(\alpha) < 1$ for all $\alpha \in \mathcal{B}$, and not all a_m belong to $\mathfrak{p}A_\mathfrak{p}$, we have $\delta < 1$. Thus, $J_\delta \subset I_\delta$ and (31) shows that $w\left(\sum_{i\in J_\delta} a_i\alpha_i\right) = \delta$. Since $w\left(\sum_{i\notin J_\delta} a_i\alpha_i\right) > \delta$, we get $w\left(\sum_{i=1}^m a_i\alpha_i\right) = \delta$, as desired. □

5.2. **Domination and similarity of prime ideals.** The aim of the Montes algorithm is to determine successive dissections of the set $\mathcal{P}$, till each prime ideal lying over $\mathfrak{p}$ is singled out. In this section, we derive from these dissections a partial ordering on a quotient of $\mathcal{P}$ by a certain equivalence relation. Needless to say, these relationships between prime ideals are not intrinsic; they depend on the choice of the polynomial $f(x) \in A[x]$ defining the extension L/K. For instance, the first dissection of $\mathcal{P}$ is determined by the factorization of $f(x)$ modulo $\mathfrak{p}$:

$$\overline{f}(y) = \prod\nolimits_\varphi \varphi(y)^{a_\varphi},$$

into a product of powers of pairwise different monic irreducible polynomials $\varphi \in \mathbb{F}_\mathfrak{p}[y]$. By Hensel's lemma, this determines a partition

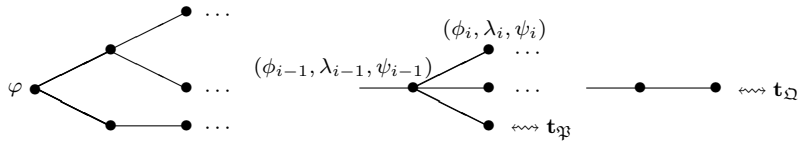
$$\mathcal{P} = \coprod\nolimits_\varphi \mathcal{P}_\varphi, \quad \mathcal{P}_\varphi := \left\{\mathfrak{P} \in \mathcal{P} \mid \overline{F}_\mathfrak{P} \text{ is a power of } \varphi\right\}.$$

Let us briefly recall how the Montes algorithm proceeds to obtain further dissections of the subsets $\mathcal{P}_\varphi$. We use the version of the algorithm described in [1, Sec. 4], guaranteeing that the OM representations $\mathbf{t}_\mathfrak{P}$ have order $r_\mathfrak{P} + 1$, where $r_\mathfrak{P}$ is the Okutsu depth of $F_\mathfrak{P}$.

For each φ, we consider initially a triple $(\mathbf{t}, \phi, \omega)$, where $\mathbf{t} = (\varphi)$ is a type of order zero, ϕ is a representative of $\mathbf{t}$ (a monic lift of φ to $A[x]$) and $\omega = \operatorname{ord}_\varphi(\overline{f})$. We submit this triple to a kind of *branching process*, by enlarging $\mathbf{t}$ to different types of higher order. This process is repeated for each branch till all OM representations of the prime ideals in $\mathcal{P}_\varphi$ are obtained. We build in this way a connected tree $\mathcal{T}_\varphi$ of OM representations, whose root node is labelled by the polynomial φ and the rest of the nodes are labelled by triples (ϕ, λ, ψ). The prime ideals of $\mathcal{P}_\varphi$ are in 1-1 correspondence with the leaves of the tree, and the type $\mathbf{t}_\mathfrak{P}$ attached to a leaf is obtained by gathering the invariants of all nodes in the unique path joining the leaf to its root node (see Figure 8).

In any iteration, the branching process is applied to a triple $(\mathbf{t}, \phi, \omega)$, where $\mathbf{t}$ is a strongly optimal type of order $i - 1 \ge 0$ dividing $f(x)$, ϕ is a representative of $\mathbf{t}$ and ω a positive integer. We compute the Newton polygon $N_i^\omega(f) \subset N^-_{\phi,v_i}(f)$ determined by the first $\omega + 1$ coefficients of the ϕ-expansion of $f(x)$. The branches of $\mathbf{t}$ are determined by all pairs (λ, ψ), where λ runs on all slopes of the sides of

FIGURE 8. Tree $\mathcal{T}_\varphi$ of OM representations of the irreducible factors of $f(x)$ whose reduction modulo $\mathfrak{p}$ is a power of φ.



$N_i^\omega(f)$ and, for each λ, the polynomial ψ runs on all monic irreducible factors of $R_{\lambda,i}(f)$.

If $\omega = 1$, there is only one branch, and the triple (ϕ, λ, ψ) determines a leaf of $\mathcal{T}_\varphi$. If $\omega > 1$, for each branch (λ, ψ) we consider the type $\mathbf{t}_{\lambda,\psi} := (\mathbf{t}; (\phi, \lambda, \psi))$, of order i, we compute a representative $\phi_{\lambda,\psi}$ of this type, and the positive integer $\omega_{\lambda,\psi} := \mathrm{ord}_{\mathbf{t}_{\lambda,\psi}}(f)$. The following subsets of $\mathcal{P}_\varphi$:

$$\mathcal{P}_{\lambda,\psi} := \{\mathfrak{P} \in \mathcal{P}_\varphi \mid \mathbf{t}_{\lambda,\psi} \text{ divides } F_{\mathfrak{P}}\}$$

are pairwise disjoint. If $\mathbf{t}_{\lambda,\psi}$ is strongly optimal, then (ϕ, λ, ψ) labels a new node of $\mathcal{T}_\varphi$, and we submit the triple $(\mathbf{t}_{\lambda,\psi}, \phi_{\lambda,\psi}, \omega_{\lambda,\psi})$ to further branching. Otherwise, $\phi_{\lambda,\psi}$ is also a representative of $\mathbf{t}$, and we submit the triple $(\mathbf{t}, \phi_{\lambda,\psi}, \omega_{\lambda,\psi})$ to further branching; this is called a *refinement step.*

Definition 5.8. *Let $\mathcal{P}_0 := \bigcup_{\mathrm{ord}_\varphi(\overline{f})=1} \mathcal{P}_\varphi$ be the subset of $\mathcal{P}$ formed by the prime ideals singled out by the first dissection.*

In fact, if $\mathrm{ord}_\varphi(\overline{f}) = 1$, then $\mathcal{P}_\varphi = \{\mathfrak{P}\}$ consists of a single prime ideal, with $e(\mathfrak{P}/\mathfrak{p}) = 1$, $f(\mathfrak{P}/\mathfrak{p}) = \deg \varphi$. In the initial step, we have already $\omega = 1$, so that $F_{\mathfrak{P}}$ has Okutsu depth zero and the tree $\mathcal{T}_\varphi$ has only the root node and one leaf:

$$\varphi \bullet\!\!-\!\!-\!\!\bullet\ (\phi, \lambda, \psi) \ \leftsquigarrow\ \mathbf{t}_{\mathfrak{P}} = (\varphi; (\phi, \lambda, \psi))$$

Definition 5.9. *A leaf of $\mathcal{T}_\varphi$ is* isolated *if it is the unique branch of its previous node. We say that $\mathfrak{P} \in \mathcal{P}$ is* isolated *if the leaf corresponding to $\mathbf{t}_{\mathfrak{P}}$ is isolated.*

For instance, in Figure 8 the prime $\mathfrak{P}$ is non-isolated and the prime $\mathfrak{Q}$ is isolated.

Definition 5.10. *Let $\mathfrak{P}, \mathfrak{Q} \in \mathcal{P}$, $\mathfrak{P} \neq \mathfrak{Q}$. If $\psi_{0,\mathfrak{P}} = \psi_{0,\mathfrak{Q}}$ (that is, $\mathbf{t}_{\mathfrak{P}}$ and $\mathbf{t}_{\mathfrak{Q}}$ belong to the same connected tree of OM representations), we define the* index of coincidence *between $\mathbf{t}_{\mathfrak{P}}$ and $\mathbf{t}_{\mathfrak{Q}}$ as:*

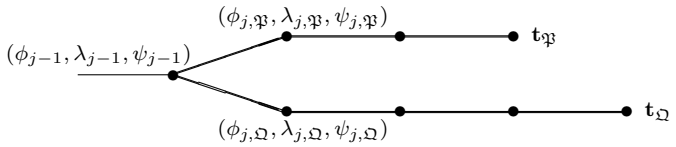
$$i(\mathbf{t}_{\mathfrak{P}}, \mathbf{t}_{\mathfrak{Q}}) = \min\{j \in \mathbb{Z}_{>0} \mid (\phi_{j,\mathfrak{P}}, \lambda_{j,\mathfrak{P}}, \psi_{j,\mathfrak{P}}) \neq (\phi_{j,\mathfrak{Q}}, \lambda_{j,\mathfrak{Q}}, \psi_{j,\mathfrak{Q}})\}.$$

If $\psi_{0,\mathfrak{P}} \neq \psi_{0,\mathfrak{Q}}$, we define $i(\mathbf{t}_{\mathfrak{P}}, \mathbf{t}_{\mathfrak{Q}}) = 0$.

By the very definition, we have:

$$i(\mathbf{t}_{\mathfrak{P}}, \mathbf{t}_{\mathfrak{Q}}) \leq \begin{cases} r_{\mathfrak{P}}, & \text{if } \mathfrak{P} \text{ is isolated,} \\ r_{\mathfrak{P}} + 1, & \text{if } \mathfrak{P} \text{ is non-isolated.} \end{cases} \tag{32}$$

If $j = i(\mathbf{t}_{\mathfrak{P}}, \mathbf{t}_{\mathfrak{Q}})$, the types $\mathbf{t}_{\mathfrak{P}}$, $\mathbf{t}_{\mathfrak{Q}}$ have the same truncation at the $(j-1)$-th order, $\mathbf{t}_{j-1} := \mathrm{Trunc}_{j-1}(\mathbf{t}_{\mathfrak{P}}) = \mathrm{Trunc}_{j-1}(\mathbf{t}_{\mathfrak{Q}})$. The last level of this type labels the first node of $\mathcal{T}_\varphi$, where the branches corresponding to the leaves $\mathbf{t}_{\mathfrak{P}}$, $\mathbf{t}_{\mathfrak{Q}}$ diverge.



The polynomials $\phi_{j,\mathfrak{P}}$, $\phi_{j,\mathfrak{Q}}$ are representatives of $\mathbf{t}_{j-1}$, but they do not necessarily coincide. Nevertheless, there exists a *greatest common ϕ-polynomial* $\phi(\mathfrak{P},\mathfrak{Q})$ of the pair $\mathbf{t}_{\mathfrak{P}}$, $\mathbf{t}_{\mathfrak{Q}}$ [8, Defn. 4.6]. The algorithm computes at some iteration a representative $\phi(\mathfrak{P},\mathfrak{Q})$ of $\mathbf{t}_{j-1}$, admitting two different branches, $(\lambda_{\mathfrak{P}}^{\mathfrak{Q}},\psi_{\mathfrak{P}}^{\mathfrak{Q}}) \neq (\lambda_{\mathfrak{Q}}^{\mathfrak{P}},\psi_{\mathfrak{Q}}^{\mathfrak{P}})$, leading, eventually after some refinement steps, to the nodes $(\phi_{j,\mathfrak{P}},\lambda_{j,\mathfrak{P}},\psi_{j,\mathfrak{P}})$, $(\phi_{j,\mathfrak{Q}},\lambda_{j,\mathfrak{Q}},\psi_{j,\mathfrak{Q}})$, respectively. The slopes $\lambda_{\mathfrak{P}}^{\mathfrak{Q}}$, $\lambda_{\mathfrak{Q}}^{\mathfrak{P}}$ are called the *hidden slopes* of the pair $\mathbf{t}_{\mathfrak{P}}$, $\mathbf{t}_{\mathfrak{Q}}$.

Let $(\mathbf{t},\phi,\omega)$ be one of the triples submitted to the branching process along the flow of the Montes algorithm, and suppose that $\omega > 1$. Recall that $\mathbf{t}$ is a strongly optimal type of order (say) $r-1 \geq 0$, and $\phi_r := \phi$ is a representative of $\mathbf{t}$. Let S be a side of $N_r^{\omega}(f) \subset N_r^{-}(f)$, $\lambda \in \mathbb{Q}^{-}$ the slope of S, and

$$R_{\lambda,r}(f)(y) \sim \psi_1(y)^{n_1} \cdots \psi_t(y)^{n_t}$$

the factorization of $R_{\lambda,r}(f)(y)$ into the product of powers of pairwise different monic irreducible polynomials in $\mathbb{F}_r[y]$. Write $\lambda = -h/e$, with h,e positive coprime integers. The length $\ell(S)$ of the side S is by definition the length of the projection of S to the horizontal axis. By Definition 3.5,

$$\ell(S) = e \deg R_{\lambda,r}(f) = e \sum\nolimits_{1\leq k\leq t} n_k \deg \psi_k.$$

Definition 5.11. *We define the* terminal length *of S as:*

$$\ell_{\mathrm{term}}(S) := e \sum\nolimits_{n_k=1} \deg \psi_k.$$

We say that S is a terminal side of order $r \geq 1$*, if $\ell_{\mathrm{term}}(S) > 0$, or equivalently, if at least one irreducible factor of $R_{\lambda,r}(f)$ divides this polynomial with exponent one.*

Let S be a terminal side of order r. Each branch (λ,ψ) of $(\mathbf{t},\phi,\omega)$, with

$$\omega_{\lambda,\psi} := \mathrm{ord}_{\mathbf{t}_{\lambda,\psi}}(f) = \mathrm{ord}_{\psi}(R_{\lambda,r}(f)) = 1,$$

singles out a prime ideal $\mathfrak{P}_{\lambda,\psi}$ of $\mathcal{P}$. In fact, $1 = \mathrm{ord}_{\mathbf{t}_{\lambda,\psi}}(f) = \sum_{\mathfrak{P}\in\mathcal{P}} \mathrm{ord}_{\mathbf{t}_{\lambda,\psi}}(F_{\mathfrak{P}})$, so that $\mathrm{ord}_{\mathbf{t}_{\lambda,\psi}}(F_{\mathfrak{P}}) = 0$ for all $\mathfrak{P} \in \mathcal{P}$, except for one prime ideal, say $\mathfrak{P}_{\lambda,\psi}$, for which $\mathrm{ord}_{\mathbf{t}_{\lambda,\psi}}(F_{\mathfrak{P}_{\lambda,\psi}}) = 1$. We denote

$$\mathcal{P}_S := \{\mathfrak{P}_{\lambda,\psi} \mid \mathrm{ord}_{\psi}(R_{\lambda,r}(f)) = 1\} \subset \mathcal{P}_{\varphi}.$$

Note that $\mathbf{t}_{\lambda,\psi}$ is simultaneously f-complete and $F_{\mathfrak{P}_{\lambda,\psi}}$-complete.

Any representative $\phi_{\lambda,\psi}$ of $\mathbf{t}_{\lambda,\psi}$ has degree $e(\deg\psi)m_r$. Hence, $\mathbf{t}_{\lambda,\psi}$ is strongly optimal if and only if $e\deg\psi > 1$; in this case, $F_{\mathfrak{P}_{\lambda,\psi}}$ has Okutsu depth $r_{\mathfrak{P}_{\lambda,\psi}} = r$, and (ϕ_r,λ,ψ) is the r-th level of the OM representation of $\mathfrak{P}_{\lambda,\psi}$. The prime ideal $\mathfrak{P}_{\lambda,\psi}$ is isolated, because $\mathbf{t}_{\lambda,\psi}$ has a unique branch, which is a leave of the tree $\mathcal{T}_{\varphi}$. This $(r+1)$-th level of $\mathbf{t}_{\mathfrak{P}_{\lambda,\psi}}$ is constructed by a last iteration applied to the triple $(\mathbf{t}_{\lambda,\psi},\phi_{\lambda,\psi},\omega_{\lambda,\psi}=1)$.

If $e\deg\psi = 1$, the Okutsu depth of $F_{\mathfrak{P}_{\lambda,\psi}}$ is $r_{\mathfrak{P}_{\lambda,\psi}} = r-1$, and $\mathfrak{P}$ is non-isolated. In fact, the iteration that constructs the leaf attached to $\mathfrak{P}_{\lambda,\psi}$ is applied to the triple $(\mathbf{t},\phi_{\lambda,\psi},\omega_{\lambda,\psi}=1)$; hence, it yields a node of level r of the tree of OM

representations. On the other hand, since $\omega > 1$, the initial triple $(\mathbf{t}, \phi_r, \omega)$ has other branches of level r.

Definition 5.12. *Let $\mathcal{S}_{\rm term}$ be the set of all terminal sides that occur along the application of the Montes algorithm to $f(x)$ and $\mathfrak{p}$. We have a partition:*

$$\mathcal{P} = \mathcal{P}_0 \cup \bigcup\nolimits_{S\in\mathcal{S}_{\rm term}} \mathcal{P}_S.$$

Let $S \in \mathcal{S}_{\rm term}$ be a terminal side of order r. If $\mathfrak{P} \in \mathcal{P}_S$, we denote $\phi_S := \phi_r$, the ϕ-polynomial from which the side S was derived. Note that $\phi_S = \phi_{r,\mathfrak{P}}$, if $\mathfrak{P}$ is isolated, but ϕ_S is not a ϕ-polynomial of $\mathbf{t}_\mathfrak{P}$, if $\mathfrak{P}$ is non-isolated.

Definition 5.13. *Let $S \in \mathcal{S}_{\rm term}$, and let $\mathfrak{P} \in \mathcal{P}_S$. We say that $\mathfrak{Q} \in \mathcal{P} \setminus \mathcal{P}_0$* dominates *$\mathfrak{P}$, and we write $\mathfrak{Q} \succ \mathfrak{P}$, if $w_\mathfrak{Q}(\phi_S(\theta)) \geq w_\mathfrak{P}(\phi_S(\theta))$.*

We say that $\mathfrak{P}, \mathfrak{Q}$ are similar*, and we write $\mathfrak{P} \simeq \mathfrak{Q}$, if $\mathfrak{Q} \succ \mathfrak{P}$ and $\mathfrak{P} \succ \mathfrak{Q}$.*

Lemma 5.14. *Let $S \in \mathcal{S}_{\rm term}$ have order r. Let $\mathfrak{P} \in \mathcal{P}_S$ and $\mathfrak{Q} \in \mathcal{P} \setminus \mathcal{P}_0$, $\mathfrak{Q} \neq \mathfrak{P}$.*

1. *$\mathfrak{Q} \succ \mathfrak{P}$ if and only if $i(\mathbf{t}_\mathfrak{P}, \mathbf{t}_\mathfrak{Q}) = r$, $\phi_S = \phi(\mathfrak{P}, \mathfrak{Q})$ and $|\lambda_\mathfrak{Q}^\mathfrak{P}| \geq |\lambda_\mathfrak{P}^\mathfrak{Q}|$.*
2. *$\mathfrak{Q} \simeq \mathfrak{P}$ if and only if $\mathfrak{Q} \in \mathcal{P}_S$.*

Proof. Let λ be the slope of S. By [7, Thm. 3.1],

$$w_\mathfrak{P}(\phi_S(\theta)) = (V_{r,\mathfrak{P}} + |\lambda|)\,/e_{0,\mathfrak{P}} \cdots e_{r-1,\mathfrak{P}}. \tag{33}$$

As mentioned above, $r = r_\mathfrak{P}$ if $\mathfrak{P}$ is isolated and $r = r_\mathfrak{P} + 1$ otherwise. By (32), $j := i(\mathbf{t}_\mathfrak{P}, \mathbf{t}_\mathfrak{Q}) \leq r$. If $j = 0$, we have $w_\mathfrak{Q}(\phi_S(\theta)) = 0$, and the claimed equivalent conditions of item 1 are both false. If $j > 0$, [8, Prop. 4.7] shows that

$$w_\mathfrak{Q}(\phi_S(\theta)) = \begin{cases} \dfrac{V_{r,\mathfrak{P}} + |\lambda_\mathfrak{Q}^\mathfrak{P}|}{e_{0,\mathfrak{P}} \cdots e_{r-1,\mathfrak{P}}}, & \text{if } j = r \text{ and } \phi(\mathfrak{P}, \mathfrak{Q}) = \phi_S, \\ \dfrac{m_{r,\mathfrak{P}}}{m_j}\,\dfrac{V_j + \min\{|\lambda_\mathfrak{P}^\mathfrak{Q}|, |\lambda_\mathfrak{Q}^\mathfrak{P}|\}}{e_0 \cdots e_{j-1}}, & \text{otherwise.} \end{cases} \tag{34}$$

The Okutsu invariants $e_0, \ldots, e_{j-1}, m_j, V_j$ of $\mathbf{t}_\mathfrak{P}$ and $\mathbf{t}_\mathfrak{Q}$ coincide, and for them we dropped the subindex $\mathfrak{P}$ or $\mathfrak{Q}$.

Suppose $j = r$ and $\phi(\mathfrak{P}, \mathfrak{Q})) = \phi_S$. We then have $\lambda_\mathfrak{P}^\mathfrak{Q} = \lambda$, by the definition of the hidden slope. By (33) and (34), $|\lambda_\mathfrak{Q}^\mathfrak{P}| \geq |\lambda_\mathfrak{P}^\mathfrak{Q}|$ is equivalent to $\mathfrak{Q} \succ \mathfrak{P}$. Therefore, in order to prove item 1 of the lemma, it is sufficient to check that $\mathfrak{Q} \succ \mathfrak{P}$ implies $j = r$ and $\phi(\mathfrak{P}, \mathfrak{Q})) = \phi_S$.

In every refinement step, the slope grows strictly in absolute size [6, Thm. 3.1]. Hence,

$$|\lambda_\mathfrak{P}^\mathfrak{Q}| \leq |\lambda_{j,\mathfrak{P}}|; \;\text{ and }\; j = r,\ \phi(\mathfrak{P}, \mathfrak{Q}) \neq \phi_S \implies |\lambda_\mathfrak{P}^\mathfrak{Q}| < |\lambda|. \tag{35}$$

If $j = r$ and $\phi(\mathfrak{P}, \mathfrak{Q}) \neq \phi_S$, then we get directly $w_\mathfrak{Q}(\phi_S(\theta)) < w_\mathfrak{P}(\phi_S(\theta))$, by (33), (34) and (35). If $j < r$, then (33), (34), (35) and the explicit recurrent formulas for V_i from section 1, show that

$$\begin{aligned} w_\mathfrak{Q}(\phi_S(\theta)) &\leq m_{r,\mathfrak{P}}\,\frac{V_j + |\lambda_{j,\mathfrak{P}}|}{m_j\, e_0 \cdots e_{j-1}} = m_{r,\mathfrak{P}}\,\frac{V_{j+1,\mathfrak{P}}}{m_{j+1,\mathfrak{P}} e_{0,\mathfrak{P}} \cdots e_{j,\mathfrak{P}}} \\ &\leq m_{r,\mathfrak{P}}\,\frac{V_{r,\mathfrak{P}}}{m_{r,\mathfrak{P}}\, e_{0,\mathfrak{P}} \cdots e_{r-1,\mathfrak{P}}} < w_\mathfrak{P}(\phi_S(\theta)). \end{aligned}$$

This ends the proof of item 1.

Let us now prove item 2. If $\mathfrak{Q} \in \mathcal{P}_S$, we have by construction $i(\mathbf{t}_\mathfrak{P}, \mathbf{t}_\mathfrak{Q}) = r$, $\phi(\mathfrak{P}, \mathfrak{Q}) = \phi_S$ and $\lambda_\mathfrak{P}^\mathfrak{Q} = \lambda_\mathfrak{Q}^\mathfrak{P} = \lambda$. Hence, $\mathfrak{Q} \succ \mathfrak{P}$ and $\mathfrak{P} \succ \mathfrak{Q}$, by the first item.

Conversely, suppose $\mathfrak{P} \simeq \mathfrak{Q}$. Let T be the terminal side for which $\mathfrak{Q} \in \mathcal{P}_T$, and let μ be the slope of T. By the first item, $i(\mathbf{t}_\mathfrak{P}, \mathbf{t}_\mathfrak{Q}) = r$, $\phi(\mathfrak{P}, \mathfrak{Q}) = \phi_S = \phi_T$, and $\lambda = \lambda_\mathfrak{P}^\mathfrak{Q} = \lambda_\mathfrak{Q}^\mathfrak{P} = \mu$. Hence, $S = T$. □

Lemma 5.15. *The relation of domination is reflexive and transitive. Thus, it induces a partial ordering on the set $(\mathcal{P} \setminus \mathcal{P}_0)/\simeq$ of similarity classes of $\mathcal{P} \setminus \mathcal{P}_0$.*

Proof. The reflexive property is obvious. Let us prove transitivity. Suppose $\mathfrak{L} \succ \mathfrak{Q}$, $\mathfrak{Q} \succ \mathfrak{P}$. Let $S, T \in \mathcal{S}_{\rm term}$ be the terminal sides such that $\mathfrak{P} \in \mathcal{P}_S$, $\mathfrak{Q} \in \mathcal{P}_T$. By Lemma 5.14, $\phi_S = \phi(\mathfrak{P}, \mathfrak{Q})$, $\phi_T = \phi(\mathfrak{Q}, \mathfrak{L})$, $r := i(\mathbf{t}_\mathfrak{P}, \mathbf{t}_\mathfrak{Q})$ is equal to $r_\mathfrak{P}$, or $r_\mathfrak{P} + 1$, according to $\mathfrak{P}$ being isolated or not, and $s := i(\mathbf{t}_\mathfrak{Q}, \mathbf{t}_\mathfrak{L})$ is equal to $r_\mathfrak{Q}$, or $r_\mathfrak{Q} + 1$, according to $\mathfrak{Q}$ being isolated or not. By (32), we have $r \leq s$, so that $i(\mathbf{t}_\mathfrak{P}, \mathbf{t}_\mathfrak{L}) = r$.

Let $(\mathbf{t}, \phi, \omega)$ be the first triple such that the three prime ideals $\mathfrak{P}, \mathfrak{Q}, \mathfrak{L}$ do not belong to the same of its branches. Let (λ, ψ) be the branch to which $\mathfrak{P}$ belongs; that is, $\mathfrak{P} \in \mathcal{P}_{\lambda,\psi}$. The prime ideal $\mathfrak{Q}$ cannot belong to the same branch. In fact, this would separate $\mathfrak{Q}$ from $\mathfrak{L}$, and we would have $\phi = \phi(\mathfrak{Q}, \mathfrak{L}) = \phi_T$; but this is impossible, because the branch of ϕ_T to which $\mathfrak{Q}$ belongs contains no other prime ideal. Therefore, $\phi = \phi(\mathfrak{P}, \mathfrak{Q}) = \phi_S$; in particular, $\mathcal{P}_{\lambda,\psi} = \{\mathfrak{P}\}$. Hence, $\mathfrak{P}$ and $\mathfrak{L}$ are also separated by this triple, and this implies $\phi(\mathfrak{P}, \mathfrak{L}) = \phi = \phi_S$.

By Lemma 5.14, in order to prove that $\mathfrak{L} \succ \mathfrak{P}$, we need only to show that $|\lambda_\mathfrak{L}^\mathfrak{P}| \geq |\lambda_\mathfrak{P}^\mathfrak{L}|$. We now have two possibilities, according to $\mathfrak{L}$, $\mathfrak{Q}$ belonging to the same branch, or to different branches.

$$\phi(\mathfrak{P},\mathfrak{Q}) \begin{cases} (\lambda,\psi) & \mathcal{P}_{\lambda,\psi} = \{\mathfrak{P}\} \\ (\lambda',\psi') & \mathfrak{Q},\, \mathfrak{L} \in \mathcal{P}_{\lambda',\psi'} \end{cases} \qquad \phi(\mathfrak{P},\mathfrak{Q}) \begin{cases} (\lambda,\psi) & \mathcal{P}_{\lambda,\psi} = \{\mathfrak{P}\} \\ (\lambda',\psi') & \mathcal{P}_{\lambda',\psi'} = \{\mathfrak{Q}\} \\ (\lambda'',\psi'') & \mathfrak{L} \in \mathcal{P}_{\lambda'',\psi''} \end{cases}$$

In the first case, we have $|\lambda_\mathfrak{L}^\mathfrak{P}| = |\lambda'| = |\lambda_\mathfrak{Q}^\mathfrak{P}| \geq |\lambda_\mathfrak{P}^\mathfrak{Q}| = |\lambda| = |\lambda_\mathfrak{P}^\mathfrak{L}|$. In the second case, the argument is similar: $|\lambda_\mathfrak{L}^\mathfrak{P}| = |\lambda_\mathfrak{L}^\mathfrak{Q}| \geq |\lambda_\mathfrak{Q}^\mathfrak{L}| = |\lambda_\mathfrak{Q}^\mathfrak{P}| \geq |\lambda_\mathfrak{P}^\mathfrak{Q}| = |\lambda_\mathfrak{P}^\mathfrak{L}|$. □

By Lemma 5.14, there is a natural bijection between $\mathcal{S}_{\rm term}$ and $(\mathcal{P} \setminus \mathcal{P}_0)/\simeq$. Therefore, domination induces a partial ordering on $\mathcal{S}_{\rm term}$ as well.

5.3. **Method of the quotients.** For each $\mathfrak{P} \in \mathcal{P}_0$, with OM representation $\mathbf{t}_\mathfrak{P} = (\psi_{0,\mathfrak{P}}; (\phi_{1,\mathfrak{P}}, \lambda_{1,\mathfrak{P}}, \psi_{1,\mathfrak{P}}))$, denote by $Q_\mathfrak{P}(x)$ the quotient of the division with remainder of $f(x)$ by $\phi_{1,\mathfrak{P}}(x)$. Consider the set:

$$\mathcal{B}_{\mathcal{P}_0} := \bigcup\nolimits_{\mathfrak{P} \in \mathcal{P}_0} \mathcal{B}_\mathfrak{P}, \quad \mathcal{B}_\mathfrak{P} := \{Q_\mathfrak{P}(\theta), \theta Q_\mathfrak{P}(\theta), \dots, \theta^{f_{0,\mathfrak{P}}-1} Q_\mathfrak{P}(\theta)\}.$$

Let S be a terminal side of order r, derived from a type

$$\mathbf{t} = (\psi_0; (\phi_1, \lambda_1, \psi_1); \cdots; (\phi_{r-1}, \lambda_{r-1}, \psi_{r-1})), \tag{36}$$

with representative ϕ_r. Denote by λ_r the slope of S. For all $1 \leq i \leq r$, let b_i be the abscissa of the right end point of the side of slope λ_i of $N_i^-(f)$. For all $0 \leq j < b_i$, let $Q_{i,j}$ be the $(b_i - j)$-th quotient of the ϕ_i-expansion of $f(x)$. Consider the set:

$$J_S := \{(j_0, \dots, j_{r-1}, j) \in \mathbb{N}^{r+1} \mid 0 \leq j_i < e_i f_i,\ 0 \leq i < r;\ 0 \leq j < \ell_{\rm term}(S)\},$$

and for any $\mathbf{j} \in J_S$, consider the element:

$$Q_\mathbf{j} := \frac{\theta^{j_0} Q'_{1,j_1}(\theta) \cdots Q'_{r-1,j_{r-1}}(\theta)\, Q_{r,j}(\theta)}{\pi^{\lfloor H'_{1,j_1} + \cdots + H'_{r-1,j_{r-1}} + H_{r,j} \rfloor}} \in B_\mathfrak{p}, \tag{37}$$

where $Q'_{i,j}$, $H'_{i,j}$ are defined in (29). Finally, let $\mathcal{B}_S := \{Q_{\mathbf{j}} \mid \mathbf{j} \in J_S\}$.

Theorem 5.16. *The following family is a $\mathfrak{p}$-reduced $\mathfrak{p}$-integral basis of B/A:*

$$\mathcal{B} := \mathcal{B}_{\mathcal{P}_0} \cup \left(\bigcup\nolimits_{S \in \mathcal{S}_{\mathrm{term}}} \mathcal{B}_S \right).$$

For the proof of the theorem we need two lemmas.

Lemma 5.17. *Let S be a terminal side of order r, derived from a type $\mathbf{t}$ with representative ϕ_r, as in (36). Let λ_r be the slope of S. For each $\mathfrak{P} \in \mathcal{P}_S$, denote by $\psi_{\mathfrak{P}} \in \mathbb{F}_r[y]$ the irreducible factor of $R_r(f)$, such that $\mathfrak{P} = \mathfrak{P}_{\lambda_r, \psi_{\mathfrak{P}}}$ is determined by the branch $(\lambda_r, \psi_{\mathfrak{P}})$.*

1. *For each $0 \le j < b_r$, $w_{\mathfrak{P}}(Q_{r,j}(\theta)) = H_{r,j}$ if and only if $\psi_{\mathfrak{P}} \nmid R_r(Q_{r,j})$.*
   If $0 \le j < \ell_{\mathrm{term}}(S)$, this condition is satisfied by at least one $\mathfrak{P} \in \mathcal{P}_S$.
2. *Let $\alpha = Q_{\mathbf{j}} \in \mathcal{B}_S$, as in (37). Then,*

$$w(\alpha) = H'_{1,j_1} + \cdots + H'_{r-1,j_{r-1}} + H_{r,j} - \lfloor H'_{1,j_1} + \cdots + H'_{r-1,j_{r-1}} + H_{r,j} \rfloor.$$

   In particular, $0 \le w(\alpha) < 1$. Moreover, for all $\mathfrak{P} \in \mathcal{P}_S$, we have $w(\alpha) = w_{\mathfrak{P}}(\alpha)$ if and only if $\psi_{\mathfrak{P}} \nmid R_r(Q_{r,j})$.
3. *Suppose that $\mathfrak{Q} \in \mathcal{P}$ either belongs to $\mathcal{P}_0$, or it does not dominate the prime ideals in $\mathcal{P}_S$. Then, $w_{\mathfrak{Q}}(\alpha) > w(\alpha)$ for all $\alpha \in \mathcal{B}_S$.*

Proof. Write $\lambda_r = -h_r/e_r$, with h_r, e_r positive coprime integers. Let $\mathfrak{P} \in \mathcal{P}_S$, and consider the type $\mathbf{t}'_{\mathfrak{P}} := \mathbf{t}_{\lambda_r, \psi_{\mathfrak{P}}} = (\mathbf{t}; (\phi_r, \lambda_r, \psi_{\mathfrak{P}}))$ dividing $F_{\mathfrak{P}}$.

The shape of $N_r^-(Q_{r,j})$ is shown in Figure 7. The ordinate H of the intersection point of the vertical axis with the line of slope λ_r that first touches $N_r^-(Q_{r,j})$ from below is equal to $y_{r,j} - (b_r - j)V_r$. By Proposition 1.5 applied to the type $\mathbf{t}'_{\mathfrak{P}}$,

$$w_{\mathfrak{P}}(Q_{r,j}(\theta)) \ge H/e_0 \cdots e_{r-1} = H_{r,j},$$

and equality holds if and only if $\psi_{\mathfrak{P}} \nmid R_r(Q_{r,j})$.

Let $\varphi := \prod_{\mathfrak{P} \in \mathcal{P}_S} \psi_{\mathfrak{P}}$, so that $\ell_{\mathrm{term}}(S) = e_r \deg \varphi$. If $0 \le j < \ell_{\mathrm{term}}(S)$, Lemma 3.6 shows that,

$$\deg R_r(Q_{r,j}) \le j/e_r < \ell_{\mathrm{term}}(S)/e_r = \deg \varphi.$$

Since φ is a separable polynomial, at least one irreducible factor $\psi_{\mathfrak{P}}$ of φ does not divide $R_r(Q_{r,j})$. This proves item 1.

Consider $\alpha = Q_{\mathbf{j}} \in \mathcal{B}_S$, as in (37). Take arbitrary prime ideals $\mathfrak{Q} \in \mathcal{P}$, $\mathfrak{P} \in \mathcal{P}_S$. By the properties of the Okutsu frame (1), $w_{\mathfrak{Q}}(\theta^{j_0}) \ge 0 = w_{\mathfrak{P}}(\theta^{j_0})$. By Theorem 3.3 and Corollary 3.7:

$$w_{\mathfrak{Q}}(Q'_{i,j_i}(\theta)) \ge H'_{i,j_i} = w_{\mathfrak{P}}(Q'_{i,j_i}(\theta)), \quad \forall\, 1 \le i < r. \tag{38}$$

By Theorem 3.3, $w_{\mathfrak{Q}}(Q_{r,j}(\theta)) \ge H_{r,j}$, and this coincides with $w_{\mathfrak{P}}(Q_{r,j}(\theta))$ if and only if $\psi_{\mathfrak{P}} \nmid R_r(Q_{r,j})$ by item 1. This proves item 2.

In order to prove item 3, it suffices to show that $w_{\mathfrak{Q}}(Q_{r,j}(\theta)) > H_{r,j}$, if $\mathfrak{Q} \in \mathcal{P}_0$ or $\mathfrak{Q} \not> \mathfrak{P}$. Let us apply Theorem 3.3 to the type $\mathbf{t}$. If $\mathfrak{Q}$ falls in cases (ii) or (iii) of the proof of the theorem, the inequalities (18) and (19) show that $w_{\mathfrak{Q}}(Q_{r,j}(\theta)) > H_{r,j}$. Suppose that $\mathfrak{Q}$ falls in case (i); that is, $\mathbf{t} \mid F_{\mathfrak{Q}}$. By (8) and Corollary 1.6,

$$w_{\mathfrak{Q}}(\phi_r(\theta)) = (V_r + |\mu|)/e_0 \cdots e_{r-1}, \quad w_{\mathfrak{P}}(\phi_r(\theta)) = (V_r + |\lambda_r|)/e_0 \cdots e_{r-1}, \tag{39}$$

where μ is one of the slopes of $N_r^-(f)$. In the notation of Definition 5.13, we have $\phi_S := \phi_r$. Thus, $\mathfrak{Q} \not> \mathfrak{P}$ means, by definition, $w_{\mathfrak{Q}}(\phi_r(\theta)) < w_{\mathfrak{P}}(\phi_r(\theta))$. By (39), we get $|\mu| < |\lambda_r|$, and by (9), we deduce that $w_{\mathfrak{Q}}(Q_{r,j}(\theta)) > H_{r,j}$. □

Definition 5.18. *We define a global $\star$-product on $B_{\mathfrak{p}} \setminus \{0\}$ by:*

$$\alpha \star \beta := \alpha\beta/\pi^{\lfloor w(\alpha\beta)\rfloor} \in B_{\mathfrak{p}}, \quad \forall\, \alpha, \beta \in B_{\mathfrak{p}}.$$

It is clearly associative and commutative.

Lemma 5.19. *Let S be a terminal side. Let $V := \prod_{\mathfrak{P}\in\mathcal{P}} \mathbb{F}_{\mathfrak{P}}$, $V_S := \prod_{\mathfrak{P}\in\mathcal{P}_S} \mathbb{F}_{\mathfrak{P}}$, and $\mathrm{pr}_S\colon V \longrightarrow V_S$ the canonical projection. Let $\mathcal{B}_{S,\delta} := \{\alpha \in \mathcal{B}_S \mid w(\alpha) = \delta\}$ for some $\delta \in w(\mathcal{B}_S)$. Then, $\mathrm{pr}_S(\mathrm{red}_\delta(\mathcal{B}_{S,\delta}))$ is an $\mathbb{F}_{\mathfrak{p}}$-basis of V_S.*

Proof. We keep the notation from Lemma 5.17. Let $\mathfrak{P} \in \mathcal{P}_S$, and denote $f_{\mathfrak{P}} := \deg \psi_{\mathfrak{P}}$. The type $\mathbf{t}'_{\mathfrak{P}} = (\mathbf{t}; (\phi_r, \lambda_r, \psi_{\mathfrak{P}}))$ is $F_{\mathfrak{P}}$-complete; hence [7, Cor. 3.8],

$$e(\mathfrak{P}/\mathfrak{p}) = e_0 \cdots e_r, \quad f(\mathfrak{P}/\mathfrak{p}) = f_0 f_1 \cdots f_{r-1} f_{\mathfrak{P}}. \tag{40}$$

For all $\mathfrak{P} \in \mathcal{P}_S$, the types $\mathbf{t}'_{\mathfrak{P}}$ coincide, except for the data involving the polynomials $\psi_{\mathfrak{P}}$. In particular, the tower of fields, $\mathbb{F}_{\mathfrak{p}} = \mathbb{F}_0 \subset \cdots \subset \mathbb{F}_r$, and the rational fractions $\pi_0, \dots, \pi_{r+1} \in K(x)$ of (21) are the same for all $\mathfrak{P} \in \mathcal{P}_S$. We denote:

$$\mathbb{F}_{\mathfrak{P}} = \mathbb{F}_r[y]/(\psi_{\mathfrak{P}}(y)) = \mathbb{F}_r[z_{\mathfrak{P}}], \quad \Pi := \Pi_{\mathfrak{P}} = \pi_{r+1}(\theta), \quad \Pi_0 := \pi_r(\theta),$$

where $z_{\mathfrak{P}}$ is the class of y in $\mathbb{F}_{\mathfrak{P}}$, so that $\psi_{\mathfrak{P}}(z_{\mathfrak{P}}) = 0$. Recall that $w_{\mathfrak{P}}(\Pi) = 1/(e_0 \cdots e_r)$, $w_{\mathfrak{P}}(\Pi_0) = 1/(e_0 \cdots e_{r-1})$ for all $\mathfrak{P} \in \mathcal{P}_S$.

Consider the set:

$$\mathcal{B}_S^0 := \left\{ \frac{\theta^{j_0} Q'_{1,j_1}(\theta) \cdots Q'_{r-1,j_{r-1}}(\theta)}{\pi^{\lfloor H'_{1,j_1} + \cdots H'_{r-1,j_{r-1}} \rfloor}} \;\middle|\; 0 \le j_i < e_i f_i,\ 0 \le i < r \right\}.$$

For all $\mathfrak{P} \in \mathcal{P}_S$, we have:

(i) $i_{\mathfrak{P}}(\mathcal{B}_S^0)$ is a level $r-1$ basis in standard form of $L_{\mathfrak{P}}/K_{\mathfrak{p}}$,
(ii) $w(\mathcal{B}_S^0) = w_{\mathfrak{P}}(\mathcal{B}_S^0) = \{t'/(e_0 \cdots e_{r-1}) \mid t' \in \mathbb{Z},\ 0 \le t' < e_0 \cdots e_{r-1}\}$.

In fact, we saw (i) along the proof of Theorem 4.11, and (ii) is deduced from (38).

Let $\delta \in w(\mathcal{B}_S)$. By Lemma 5.17, $0 \le \delta < 1$ and there exists $\mathfrak{P} \in \mathcal{P}_S$ such that $\delta \in w_{\mathfrak{P}}(L^*) = (e_0 \cdots e_r)^{-1}\mathbb{Z}$. Thus, $\delta = t/(e_0 \cdots e_r)$ for some integer $0 \le t < e_0 \cdots e_r$. Let q_t be the unique integer, $0 \le q_t < e_r$, such that $q_t h_r \equiv t \pmod{e_r}$. For any $0 \le j < \ell_{\mathrm{term}}(S)$, the argument of the proof of item (a) of Lemma 4.9 shows that:

$$j \not\equiv q_t \pmod{e_r} \implies H_{r,j} + t'/(e_0 \cdots e_{r-1}) \not\equiv \delta \pmod{\mathbb{Z}},$$

for all integers $0 \le t' < e_0 \cdots e_{r-1}$, whereas

$$j = q_t + k e_r \implies H_{r,j} + t_k/(e_0 \cdots e_{r-1}) \equiv \delta \pmod{\mathbb{Z}},$$

for a uniquely determined integer $0 \le t_k < e_0 \cdots e_{r-1}$. This leads to:

$$\mathcal{B}_{S,\delta} = \bigcup\nolimits_{0 \le k < f_S} Q_{r,q_t+ke_r}(\theta) \star \mathcal{B}^0_{S,t_k},$$

where $f_S := \sum_{\mathfrak{P}\in\mathcal{P}_S} f_{\mathfrak{P}} = \ell_{\mathrm{term}}(S)/e_r = \dim_{\mathbb{F}_r} V_S$ and $\mathcal{B}^0_{S,t_k}$ is the subset of $\mathcal{B}_S^0$ formed by those α^0 such that $w(\alpha^0) = t_k/e_0 \cdots e_{r-1}$.

For any $0 \le k < f_S$, write $\mathcal{B}^0_{S,t_k} = \Pi_0^{t_k} U_k$, for $U_k \subset L$. By condition (i) above, $\mathrm{red}_{L_{\mathfrak{P}}}(i_{\mathfrak{P}}(U_k)) \subset \mathbb{F}_r$ is an $\mathbb{F}_{\mathfrak{p}}$-basis of $\mathbb{F}_r$ for all $\mathfrak{P} \in \mathcal{P}_S$. Now, the elements in $\mathcal{B}_{S,\delta}$ may be parameterized as:

$$\alpha_{k,u} = Q_{r,j}(\theta) \star \Pi_0^{t_k} u, \quad 0 \le k < f_S,\ u \in U_k,$$

for $j = q_t + ke_r$. Let us compute the $\mathfrak{P}$-th component $\mathrm{red}_{L_\mathfrak{P}}(i_\mathfrak{P}(\alpha_{k,u}/\Pi^t))$ of $\mathrm{red}_\delta(\alpha_{k,u}) \in V$ for all $\mathfrak{P} \in \mathcal{P}_S$. By item 2 of Lemma 5.17:

$$w(\alpha_{k,u}) = w_\mathfrak{P}(\alpha_{k,u}) \iff \psi_\mathfrak{P} \nmid R_r(Q_{r,j}) \iff R_r(Q_{r,j})(z_\mathfrak{P}) \neq 0. \tag{41}$$

If $\mathfrak{P}$ satisfies (41), then $i_\mathfrak{P}$ is compatible with the global and local $\star$ operations, and the arguments of the proof of Proposition 4.10 lead to (28) and:

$$\begin{aligned}\eta_{k,u,\mathfrak{P}} &:= \mathrm{red}_{L_\mathfrak{P}}(i_\mathfrak{P}(\alpha_{k,u}/\Pi^t)) = \mathrm{red}_{L_\mathfrak{P}}(i_\mathfrak{P}(Q_{r,j}(\theta) \star \Pi_0^{t_k} u\, \Pi^{-t})) \\ &= \mathrm{red}_{L_\mathfrak{P}}(i_\mathfrak{P}(Q_{r,j}(\theta)) \star i_\mathfrak{P}(\Pi_0)^{t_k} i_\mathfrak{P}(\Pi)^{-t})\, \bar{u} \\ &= R_r(Q_{r,j})(z_\mathfrak{P}) \cdot \tau_k \cdot (z_\mathfrak{P})^{N+k-d_k}\, \bar{u} \\ &= \zeta_k \cdot (z_\mathfrak{P})^N (C_{d_k}(z_\mathfrak{P})^{k-d_k} + \cdots + C_0(z_\mathfrak{P})^k)\, \bar{u},\end{aligned}$$

where $\bar{u} := \mathrm{red}_{L_\mathfrak{P}}(i_\mathfrak{P}(u))$, $d_k = \deg R_r(Q_{r,j}) \leq k$, $\tau_k, \zeta_k, C_0, C_{d_k} \in \mathbb{F}_r^*$, $C_i \in \mathbb{F}_r$ for $i \neq 0, d_k$, and N is an integer that depends only on t (that is, on δ).

If $\mathfrak{P}$ does not satisfy (41), then $w_\mathfrak{P}(\alpha_{k,u}) > w(\alpha_{k,u})$, so that $\eta_{k,u,\mathfrak{P}} = 0$. Since $R_r(Q_{r,j})(z_\mathfrak{P}) = 0$ in this case, the above formula for $\eta_{k,u,\mathfrak{P}}$ holds for all $\mathfrak{P} \in \mathcal{P}_S$.

Our aim is to show that the vectors $\eta_{k,u} := (\eta_{k,u,\mathfrak{P}})_{\mathfrak{P}\in\mathcal{P}_S} \in V_S$ for $0 \leq k < f_S$ and $u \in U_k$, are an $\mathbb{F}_\mathfrak{p}$-basis of V_S. Clearly, the map:

$$(x_\mathfrak{P})_{\mathfrak{P}\in\mathcal{P}_S} \mapsto ((C_0)^{-1}(z_\mathfrak{P})^{-N} x_\mathfrak{P})_{\mathfrak{P}\in\mathcal{P}_S}$$

is an $\mathbb{F}_\mathfrak{p}$-automorphism of V_S. Thus, since $\bar{u}, \zeta_k \in \mathbb{F}_r^*$ do not depend on $\mathfrak{P} \in \mathcal{P}_S$, we may assume that

$$\eta_{k,u} = \bar{u} \cdot \zeta_k \cdot \eta_k, \quad \eta_k = \big(c_{d_k}(z_\mathfrak{P})^{k-d_k} + \cdots + c_1(z_\mathfrak{P})^{k-1} + (z_\mathfrak{P})^k\big)_{\mathfrak{P}\in\mathcal{P}_S} \in V_S,$$

where $c_i := C_i/C_0$ for all i. Since for all k the family $\{\bar{u} \mid u \in U_k\}$ is an $\mathbb{F}_\mathfrak{p}$-basis of $\mathbb{F}_r$, it suffices to check that the family of all $\{\zeta_k\eta_k \mid 0 \leq k < f_S\}$ is an $\mathbb{F}_r$-basis of V_S. Since $\dim_{\mathbb{F}_r} V_S = f_S$ and all ζ_k belong to $\mathbb{F}_r^*$, this is equivalent to $\{\eta_k \mid 0 \leq k < f_S\}$ being an $\mathbb{F}_r$-linearly independent family of V_S. We can relate this family to the family $\eta'_k := ((z_\mathfrak{P})^k)_{\mathfrak{P}\in\mathcal{P}_S}$ by the following equations:

$$\eta_k = \eta'_k + c_1\eta'_{k-1} + \cdots + c_{d_k}\eta'_{k-d_k}.$$

Since the transition matrix between the two families is invertible, it suffices to check that the family $\{\eta'_k \mid 0 \leq k < f_S\}$ is $\mathbb{F}_r$-linearly independent. Now, a linear relation of the form: $\sum_{0\leq k<f_S} a_k\eta'_k = 0$, with $a_k \in \mathbb{F}_r$, is equivalent to:

$$\sum\nolimits_{0\leq k<f_S} a_k(z_\mathfrak{P})^k = 0, \quad \forall\, \mathfrak{P} \in \mathcal{P}_S.$$

Since the irreducible polynomials $\psi_\mathfrak{P}$, for $\mathfrak{P} \in \mathcal{P}_S$, are pairwise different, this implies that the polynomial $\sum_{0\leq k<f_S} a_k x^k$ is divisible by the polynomial $\prod_{\mathfrak{P}\in\mathcal{P}_S} \psi_\mathfrak{P}$, which has degree f_S. This occurs only when all coefficients a_k vanish. □

Proof of Theorem 5.16. Denote $n_\mathfrak{P} = e(\mathfrak{P}/\mathfrak{p})f(\mathfrak{P}/\mathfrak{p})$ for all $\mathfrak{P} \in \mathcal{P}$. Clearly,

$$\#\mathcal{B}_{\mathcal{P}_0} = \sum\nolimits_{\mathfrak{P}\in\mathcal{P}_0} f_{0,\mathfrak{P}} = \sum\nolimits_{\mathfrak{P}\in\mathcal{P}_0} n_\mathfrak{P}.$$

On the other hand, by (40), for any $S \in \mathcal{S}_{\mathrm{term}}$,

$$\begin{aligned}\#\mathcal{B}_S &= (e_0f_0)\cdots(e_{r-1}f_{r-1})\, \ell_{\mathrm{term}}(S) \\ &= (e_0f_0)\cdots(e_{r-1}f_{r-1}) \cdot e_r \cdot \sum\nolimits_{\mathfrak{P}\in\mathcal{P}_S} f_\mathfrak{P} = \sum\nolimits_{\mathfrak{P}\in\mathcal{P}_S} n_\mathfrak{P}.\end{aligned}$$

Thus, by Lemma 5.12, $\#\mathcal{B} = \sum_{\mathfrak{P}\in\mathcal{P}} n_\mathfrak{P} = n$. Also, $\mathcal{B} \subset B_\mathfrak{p}$ by construction.

For any $\mathfrak{P} \in \mathcal{P}_0$, Corollary 3.7 shows that $w_{\mathfrak{P}}(Q_{\mathfrak{P}}(\theta)) = 0$, and equation (1) shows that $w_{\mathfrak{P}}(\theta^j) = 0$, for all $0 \le j < f_{0,\mathfrak{P}}$; hence, $w(\alpha) = 0$ for all $\alpha \in \mathcal{B}_{\mathcal{P}_0}$. We conclude that $0 \le w(\alpha) < 1$, for all $\alpha \in \mathcal{B}$, by

item 2 of Lemma 5.17. Therefore, by Lemma 5.6, we need only to check that the set $\mathcal{B}$ is reduced. To this end, we apply the criterion of Lemma 5.7.

For any $\delta \in w(\mathcal{B})$, let $\mathcal{B}_{S,\delta} := \mathcal{B}_\delta \cap \mathcal{B}_S$. The set $\mathcal{B}_\delta$ splits into the disjoint union:

$$\mathcal{B}_\delta = \begin{cases} \mathcal{B}_{\mathcal{P}_0} \cup \left(\bigcup_{S\in\mathcal{S}_{\rm term}} \mathcal{B}_{S,\delta}\right), & \text{if } \delta = 0, \\ \bigcup_{S\in\mathcal{S}_{\rm term}} \mathcal{B}_{S,\delta}, & \text{if } \delta > 0. \end{cases}$$

Our aim is to prove the $\mathbb{F}_{\mathfrak{p}}$-linear independence of the family $\mathrm{red}_\delta(\mathcal{B}_\delta)$, for all $\delta \in w(\mathcal{B})$. Let us show first that the family $\bigcup_{S\in\mathcal{S}_{\rm term}} \mathrm{red}_\delta\left(\mathcal{B}_{S,\delta}\right)$ is linearly independent.

Take any $\delta \in w(\mathcal{B})$. Let $\mathcal{S}_\delta := \{S \in \mathcal{S}_{\rm term} \mid \mathcal{B}_{S,\delta} \neq \emptyset\}$. For any $S \in \mathcal{S}_\delta$, write: $\mathrm{red}_\delta(\mathcal{B}_{S,\delta}) = \{\zeta_{m,S} \mid 1 \le m \le n_{S,\delta}\} \subset V$.

Suppose that for some family of elements $a_{m,S} \in \mathbb{F}_{\mathfrak{p}}$, we have

$$\sum\nolimits_{m,S} a_{m,S}\,\zeta_{m,S} = 0, \tag{42}$$

the sum running on $S \in \mathcal{S}_\delta$ and $1 \le m \le n_{S,\delta}$. Take $T \in \mathcal{S}_\delta$ minimal with respect to the relationship of domination (cf. the remark following Lemma 5.15); that is:

$$\mathfrak{Q} \not> \mathfrak{P},\ \forall\, \mathfrak{Q} \in \mathcal{P}_T,\ \forall\, \mathfrak{P} \in \mathcal{P}_S,\ \forall\, S \in \mathcal{S}_\delta,\ S \neq T.$$

By item 3 of Lemma 5.17,

$$w_{\mathfrak{Q}}(\alpha) > \delta, \quad \forall\, \mathfrak{Q} \in \mathcal{P}_T,\ \forall\, \alpha \in \mathcal{B}_{S,\delta},\ \forall\, S \in \mathcal{S}_\delta,\ S \neq T.$$

Hence, $\mathrm{pr}_T(\zeta_{m,S}) = 0$, for all $S \in \mathcal{S}_\delta$, $S \neq T$, and all m. Thus, if we apply pr_T to both sides of (42), we get

$$\sum\nolimits_m a_{m,T}\,\mathrm{pr}_T(\zeta_{m,T}) = 0,$$

and by Lemma 5.19, $a_{m,T} = 0$, for all m. Thus, we get again an equation like (42), for S running on the set $\mathcal{S}_\delta \backslash \{T\}$. By applying in a recurrent way the same argument, we conclude that $a_{m,S} = 0$ for all m, S. Therefore, the family $\bigcup_{S\in\mathcal{S}_{\rm term}} \mathrm{red}_\delta\left(\mathcal{B}_{S,\delta}\right)$ is $\mathbb{F}_{\mathfrak{p}}$-linearly independent.

This proves the theorem in the case $\delta > 0$. Suppose now $\delta = 0$.

Define the *support* of a vector $(x_{\mathfrak{P}})_{\mathfrak{P}\in\mathcal{P}} \in V$, as the set of indices $\mathfrak{P} \in \mathcal{P}$ such that $x_{\mathfrak{P}} \neq 0$. For each $\mathfrak{P} \in \mathcal{P}_0$, $\mathrm{red}_0(\mathcal{B}_{\mathfrak{P}})$ is an $\mathbb{F}_{\mathfrak{p}}$-linearly independent subset of V, and all these vectors have support $\{\mathfrak{P}\}$, because $w_{\mathfrak{Q}}(Q_{\mathfrak{P}}) > 0$, for all $\mathfrak{Q} \in \mathcal{P}$, $\mathfrak{Q} \neq \mathfrak{P}$. In fact, since $\psi_{0,\mathfrak{Q}} \neq \psi_{0,\mathfrak{P}}$, the prime ideal $\mathfrak{Q}$ falls in case (iii) of Theorem 3.3, applied to the type of order zero $\mathbf{t} = (\psi_{0,\mathfrak{P}})$, with representative $\phi_{1,\mathfrak{P}}$.

We have seen that the subset $\bigcup_{S\in\mathcal{S}_{\rm term}} \mathrm{red}_0\left(\mathcal{B}_{S,0}\right)$ is $\mathbb{F}_{\mathfrak{p}}$-linearly independent. All these vectors in V have support contained in $\mathcal{P} \setminus \mathcal{P}_0$, by item 3 of Lemma 5.17. Therefore, $\mathrm{red}_0(\mathcal{B}_0)$ is $\mathbb{F}_{\mathfrak{p}}$-linearly independent because it is the union of linearly independent subsets with pairwise disjoint supports. □

6. An algorithm for the computation of $\mathfrak{p}$-integral bases

6.1. **The algorithm.** In this section, we describe in pseudo-code an algorithm based on the method of the quotients as presented in Theorem 5.16.

We denote by $\phi_i^{\mathbf{t}}$, $\lambda_i^{\mathbf{t}}$, $\psi_i^{\mathbf{t}}$ etc. the data at the i-th level of a type $\mathbf{t}$. Also, with the notation of (29), we store at the first level of $\mathbf{t}$ two lists $\texttt{ProdQ}^{\mathbf{t}}$, $\texttt{ProdQVals}^{\mathbf{t}}$ containing a partial product of quotients $Q'_{i,j}$ and the corresponding sums of the rational numbers $H'_{i,j}$, respectively.

The order of a type $\mathbf{t}$ is the largest level i for which all three fundamental invariants $(\phi_i, \lambda_i, \psi_i)$ are assigned.

Method of the quotients

INPUT:
- A monic irreducible separable polynomial $f \in A[x]$.
- A non-zero prime ideal $\mathfrak{p}$ of A.

1 Initialize empty lists `BasisNums`, `BasisDens`.

2 Factorize $\overline{f}$ in $\mathbb{F}[y]$.

3 FOR each monic irreducible factor φ of $\overline{f}$ DO

4 Take a monic lift $\phi \in A[x]$ of φ.

5 IF $\operatorname{ord}_\varphi(\overline{f}) = 1$ THEN

(a) Set $Q, a \leftarrow \operatorname{quotrem}(f, \phi)$.

(b) Join $[Q(x)x^k \mid 0 \le k < \deg\varphi]$ to the list `BasisNums`.
Join $[0 \mid 0 \le k < \deg\varphi]$ to the list `BasisDens`.

(c) CONTINUE to the next irreducible factor φ.

6 Initialize the list `Types=[t]`, where $\mathbf{t}$ is a type of order zero with
$\psi_0^{\mathbf{t}} \leftarrow \varphi, \quad \omega_1^{\mathbf{t}} \leftarrow \operatorname{ord}_\varphi \overline{f}, \quad \phi_1^{\mathbf{t}} \leftarrow \phi,$
$\texttt{ProdQ}^{\mathbf{t}} \leftarrow [x^k \mid 0 \le k < \deg\varphi], \quad \texttt{ProdQVals}^{\mathbf{t}} \leftarrow [0 \mid 0 \le k < \deg\varphi].$
WHILE #`Types` > 0 **DO**

7 Extract (and delete) the last type $\mathbf{t}_0$ from `Types`. Let $i-1$ be its order and set $L \leftarrow \#\texttt{ProdQ}^{\mathbf{t}_0}$.

8 For $\omega_i = \omega_i^{\mathbf{t}_0}$, compute the coefficients $a_0, \dots, a_{\omega_i}$ of the $\phi_i^{\mathbf{t}_0}$-expansion of f and store the $\phi_i^{\mathbf{t}_0}$-quotients $\texttt{Quots} \leftarrow [Q_1, \dots, Q_{\omega_i}]$.

9 Compute the Newton polygon $N_i^{\omega_i}(f)$ and the rational numbers $\texttt{QuotsVals} \leftarrow [H_1, \dots, H_{\omega_i}]$ considered in Theorem 3.3.

10 FOR every side S of $N_i^{\omega_i}(f)$ DO

11 Set $\lambda_i^{\mathbf{t}_0} \leftarrow$ slope of S, $\quad e_i \leftarrow$ denominator of $|\lambda_i^{\mathbf{t}_0}|$.

12 Compute the residual polynomial $R_i(f)$ and factorize it in $\mathbb{F}_i[y]$.

13 $\ell_{\mathrm{term}}(S) \leftarrow e_i \sum_{\operatorname{ord}_\psi R_i(f)=1} \deg\psi$,
$J \leftarrow \max\{\ell_{\mathrm{term}}(S), \max_\psi\{e_i \deg\psi\}\}$,
where ψ runs on the irreducible factors of $R_i(f)$.

14 For b being the abscissa of the right end point of S, compute two lists:
$\texttt{Enlarge} \leftarrow [\texttt{Quots}[b-j]\texttt{*P} \mid 1 \le j \le J,\ \texttt{P} \in \texttt{ProdQ}^{\mathbf{t}_0}]$
$\texttt{EnlargeVals} \leftarrow [\texttt{QuotsVals}[b-j]\texttt{+H} \mid 1 \le j \le J,\ \texttt{H} \in \texttt{ProdQVals}^{\mathbf{t}_0}]$.

15 Join $\texttt{Enlarge}[1..\ell_{\mathrm{term}}(S)L]$ to the list `BasisNums`.
Join $\texttt{EnlargeVals}[1..\ell_{\mathrm{term}}(S)L]$ to the list `BasisDens`.

16 FOR every monic irreducible factor ψ with $\operatorname{ord}_\psi R_i(f) > 1$ DO

(a) Set $\mathbf{t} \leftarrow \mathbf{t}_0$ and extend $\mathbf{t}$ to an order i type by setting $\psi_i^{\mathbf{t}} \leftarrow \psi$.

(b) Compute a representative ϕ of $\mathbf{t}$.

(c) IF $\deg\phi = \deg\phi_i^{\mathbf{t}}$ THEN

(c1) Set $\phi_i^{\mathbf{t}} \leftarrow \phi$, $\omega_i^{\mathbf{t}} \leftarrow \operatorname{ord}_\psi R_i(f)$, and consider again $\mathbf{t}$ as a type of order $i-1$ by erasing the value of $\psi_i^{\mathbf{t}}$.

ELSE

(c2) Set $\phi_{i+1}^{\mathbf{t}} \leftarrow \phi$, $\omega_{i+1}^{\mathbf{t}} \leftarrow \operatorname{ord}_\psi R_i(f)$, $L' \leftarrow e_i(\deg\psi)L$.

(c3) Join $\texttt{Enlarge}[L+1\,..\,L']$ to the list $\texttt{ProdQ}^{\mathbf{t}}$.

Join $\texttt{EnlargeVals}[L+1\,..\,L']$ to the list $\texttt{ProdQVals}^{\mathbf{t}}$.

17 Include $\mathbf{t}$ as a new member of the list `Types`.

END WHILE

OUTPUT:

– A $\mathfrak{p}$-reduced $\mathfrak{p}$-integral basis of B/A, where B is the integral closure of A in $K[x]/(f)$. For $1 \le i \le \deg f$, the i-th member of the basis is $\pi^{-\lfloor \nu_i \rfloor} g_i(x) \pmod{f(x)}$, where $g_i(x) =$`BasisNums[`i`]` and $\nu_i =$`BasisDens[`i`]`.

Remarks. (1) The set $\mathcal{B}_{\mathcal{P}_0}$ from Theorem 5.16 is computed by the instructions **5**(b) for the different irreducible factors φ dividing $\overline{f}$ with exponent one.

(2) The Newton polygon $N_i^{\omega_i}(f)$ in **9** is the lower convex hull of the set of points $\left(j, v_i^{\mathbf{t}_0}(a_j(\phi_i^{\mathbf{t}_0})^j\right)$ for $0 \le j \le \omega_i$.

(3) For a given side S of the Newton polygon, the list `Enlarge` in **14** computes the new products of quotients involving quotients of level i. The index J defined in **13** controls the minimum number of products that are needed. If S is terminal, the first $\ell_{\text{term}}(S)L$ products in that list are the numerators of the members of the $\mathfrak{p}$-integral basis corresponding to the subset $\mathcal{B}_S$, as defined in (37). Note that we multiply the quotients $Q_{i,j}$ of the last level $r := i$, contained in the list `Quots`, by some products of quotients $Q'_{i',j}$ of level $i' < r = i$, contained in the list $\texttt{ProdQ}^{\mathbf{t}_0}$.

(4) When one of the branches $\mathbf{t}$ of the analyzed type $\mathbf{t}_0$ is strongly optimal, we actualize the value of $\texttt{ProdQ}^{\mathbf{t}}$ in **16**(c3). Since we store in this list the products of the quotients $Q'_{i,j}$ introduced in (29), we must replace $Q_{r,0}$ by $Q'_{r,0} = 1$; this amounts to joining $\texttt{Enlarge}[L+1\,..\,L']$ to the old list $\texttt{ProdQ}^{\mathbf{t}}$.

6.2. **Complexity analysis.** Denote $\delta := v_{\mathfrak{p}}(\operatorname{Disc}(f))$. If $\delta = 0$, then $B_{\mathfrak{p}} = A_{\mathfrak{p}}[\theta]$; thus, we assume $\delta > 0$ in our analysis. By [1, Thm. 3.14], for the computation of a $\mathfrak{p}$-integral basis of B/A we may work modulo $\mathfrak{p}^{\delta+1}$. Hence, we assume that the elements of A are finite π-adic developments of length $\delta+1$.

Definition 6.1. *An operation in A is called* $\mathfrak{p}$-small *if it involves two elements belonging to a fixed system of representatives of $A/\mathfrak{p}$.*

Each multiplication in A costs $O(\delta^{1+\epsilon})$ $\mathfrak{p}$-small operations, if we assume the fast multiplications techniques of Schönhage-Strassen [21]. Also, if $q := \#A/\mathfrak{p}$, a $\mathfrak{p}$-small operation in A requires $O\left(\log(q)^{1+\epsilon}\right)$ word operations, the cost of an operation in the residue field $A/\mathfrak{p}$.

The Montes algorithm has a cost of $O\left(n^{2+\epsilon} + n^{1+\epsilon}\delta\log q + n^{1+\epsilon}\delta^{2+\epsilon}\right)$ $\mathfrak{p}$-small operations [1, Thm. 5.15]. Let us estimate the cost of the extra tasks that are necessary to compute the $\mathfrak{p}$-integral basis. The computation of $\mathcal{B}_{\mathcal{P}_0}$ being negligible, let us discuss the computation of $\bigcup_{S\in\mathcal{S}_{\text{term}}} \mathcal{B}_S$.

For any element $\alpha \in \mathcal{B}_S$, the factors $Q_{i,j}$ of the numerator of α and the summands $H_{i,j}$ of the exponent of the denominator are computed along the flow of the Montes

algorithm. In the computation of α we may neglect the computation of the sum of the $H_{i,j}$ and the final division by a power of π.

Suppose S is a terminal side of order r derived from a type $\mathbf{t}$ of order $r-1$, with representative ϕ_r. We compute $\mathcal{B}_S$ in r steps:

$$\mathcal{B}_{S,0} = \{1, \theta, \dots, \theta^{f_0-1}\}, \quad \mathcal{B}_{S,i} = \bigcup\nolimits_{0\le j<e_i f_i} Q'_{i,j}(\theta) \star \mathcal{B}_{S,i-1},\ 1 \le i < r,$$

and finally, $\mathcal{B}_S = \mathcal{B}_{S,r} = \bigcup_{0\le j<e_r f_S} Q_{r,j}(\theta) \star \mathcal{B}_{S,r-1}$. Clearly,

$$\begin{aligned} &\#\mathcal{B}_{S,i} = (e_0 f_0)\cdots(e_i f_i), \quad 0 \le i < r, \\ &n_S := \#\mathcal{B}_{S,r} = (e_0 f_0)\cdots(e_{r-1} f_{r-1}) e_r f_S = \textstyle\sum_{\mathfrak{P}\in\mathcal{P}_S} n_{\mathfrak{P}}. \end{aligned}$$

If we keep only the numerators in mind, each element of $\mathcal{B}_{S,i}$, $i \ge 1$, is obtained after one multiplication in $A[\theta]$: $Q'_{i,j}(\theta)$ or $Q_{r,j}(\theta)$ times an element in $\mathcal{B}_{S,i-1}$. Thus, the total number of multiplications for the computation of $\mathcal{B}_S$ is:

$$N = e_0 f_0 + (e_0 f_0)(e_1 f_1) + \cdots + (e_0 f_0)\cdots(e_{r-1} f_{r-1}) + (e_0 f_0)\cdots(e_{r-1} f_{r-1})(e_r f_S).$$

Now, since the type $\mathbf{t}$ is optimal, we have $e_i f_i \ge 2$, for $1 \le i < r$. Thus,

$$N \le \frac{n_S}{2^{r-1}} + \frac{n_S}{2^{r-2}} + \cdots + \frac{n_S}{1} + n_S = n_S(1 + 2 - 2^{1-r}) \le 3n_S.$$

Since $n \ge \sum_{S\in\mathcal{S}_{\mathrm{term}}} n_S$, the total number of multiplications in $A[\theta]$ required for the computation of $\mathcal{B}$ is $O(n)$. Since each multiplication in $A[\theta]$ has a cost of $O(n^{1+\epsilon})$ multiplications in A, the total cost of these $O(n)$ multiplications in $A[\theta]$ is $O\left(n^{2+\epsilon}\delta^{1+\epsilon}\right)$ $\mathfrak{p}$-small operations. By adding this cost to the cost of the Montes algorithm, we get the following total estimation.

Theorem 6.2. *The computation of a $\mathfrak{p}$-integral basis of B/A requires not more than $O\left(n^{2+\epsilon}\delta^{1+\epsilon} + n^{1+\epsilon}\delta\log q + n^{1+\epsilon}\delta^{2+\epsilon}\right)$ $\mathfrak{p}$-small operations in A. If $A/\mathfrak{p}$ is small, we obtain an estimation of $O\left(n^{2+\epsilon}\delta^{1+\epsilon} + n^{1+\epsilon}\delta^{2+\epsilon}\right)$ word operations.*

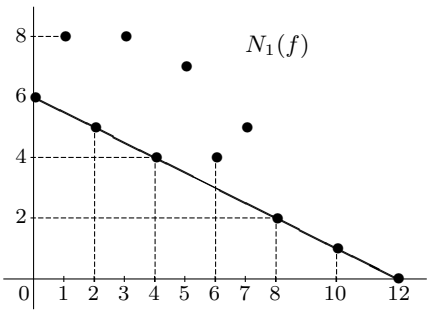
This cost is clearly lower than the cost of the OM method from section 2. Besides the application of the Montes algorithm and the $O(n)$ multiplications in $A[\theta]$ required for the construction of the $\mathfrak{p}$-integral basis, the OM method had the extra cost of computing sufficiently good aproximations to each of the irreducible factors of $f(x)$ over $\mathcal{O}_{\mathfrak{p}}$.

Also, an optimal method based on the Round 2 or Round 4 techniques would have the cost of $\mathfrak{p}$-adic factorization plus (at least) $O(n)$ multiplications in $A[\theta]$. The best estimations for the cost of $\mathfrak{p}$-adic factorization based on those methods are of $O\left(n^{3+\epsilon}\delta^{1+\epsilon} + n^{2+\epsilon}\delta^{2+\epsilon}\right)$ $\mathfrak{p}$-small operations [19].

6.3. **An example.** Let us show how the method of the quotients works with an example. Take $A = \mathbb{Z}$, $\mathfrak{p} = 2\mathbb{Z}$ and

$$f(x) = x^{12} + 14x^{10} + 60x^8 + 32x^7 + 80x^6 + 128x^5 - 80x^4 + 256x^3 - 288x^2 - 256x + 832.$$

Since $f(x) \equiv x^{12} \pmod 2$, there will be only one tree of types, whose root node is the type of order zero $\mathbf{t}_0 = (y)$, determined by the irreducible polynomial $\psi_0(y) = y$. Take $\phi_1(x) = x$ as a representative of this type. The Newton polygon $N_1(f)$ is one-sided of slope $-1/2$.



The residual polynomial of the first order attached to the side $S = N_1(f)$ is:

$$R_{-1/2,1}(f)(y) = y^6 + y^5 + y^4 + y^2 + y + 1 = (y^2 + y + 1)(y + 1)^4.$$

Thus, the type $\mathbf{t}_0$ ramifies into two types of order one:

$$\mathbf{t}_1 = (y; (x, -1/2, y^2 + y + 1)), \quad \mathbf{t}_1' = (y; (x, -1/2, y + 1)).$$

Since $y^2 + y + 1$ divides $R_{-1/2,1}(f)(y)$ with exponent one, the type $\mathbf{t}_1$ is f-complete and S is a terminal side of order 1, with $\ell_{\text{term}}(S) = 4$. The type $\mathbf{t}_1$ singles out a prime ideal $\mathfrak{P}$ with $e(\mathfrak{P}/p) = f(\mathfrak{P}/p) = 2$. If $Q_1, \dots, Q_{12}$ are the twelve quotients of the x-adic development of $f(x)$, we have:

$$\begin{array}{llll} Q_{1,0} = Q_{12} = 1, & H_{1,0} = 0, & Q_{1,1} = Q_{11} = x, & H_{1,1} = 1/2, \\ Q_{1,2} = Q_{10} = x^2 + 14, & H_{1,2} = 1, & Q_{1,3} = Q_9 = x^3 + 14x, & H_{1,3} = 3/2. \end{array}$$

The set $\mathcal{B}_S$ contains the following four globally integral elements:

$$\mathcal{B}_S = \left\{1,\ \theta,\ (\theta^2 + 14)/2,\ (\theta^3 + 14\theta)/2\right\}.$$

The type $\mathbf{t}_1'$ is not complete and its analysis requires some more work in order two. Before analyzing its branching, we store a list $\mathcal{B}_1 = \{1, \theta\}$ with the quotients $Q_{1,j}'$ for $0 \le j < e_1 f_1 = 2$, and also the corresponding values $H_{1,0}' = 0$, $H_{1,1}' = 1/2$. All future branches of $\mathbf{t}_1'$ will share these data.

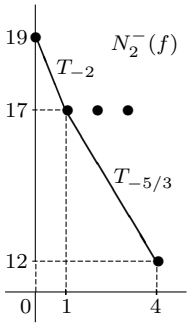
Let us choose $\phi_2(x) = x^2 + 2$ as a representative of $\mathbf{t}_1'$. By Lemma 1.4, $\ell(N_2^-(f)) = \operatorname{ord}_{\mathbf{t}_1'}(f) = 4$; thus, we compute the ϕ_2-expansion of $f(x)$ only up to degree four:

$$f(x) = 1024 - 512x + 128x\phi_2(x) - 64x\phi_2(x)^2 + 32x\phi_2(x)^3 - 20\phi_2(x)^4 + \dots.$$

The first four quotients of this ϕ_2-development are:

$$\begin{aligned} Q_1 &= x^{10} + 12x^8 + 36x^6 + 32x^5 + 8x^4 + 64x^3 - 96x^2 + 128x - 96, \\ Q_2 &= x^8 + 10x^6 + 16x^4 + 32x^3 - 24x^2 - 48, \\ Q_3 &= x^6 + 8x^4 + 32x - 24, \\ Q_4 &= x^4 + 6x^2 - 12. \end{aligned}$$

Since $V_2 = v_2(\phi_2) = 2 = v_2(2)$ and $v_2(x) = 1$, we get $v_2(1024 - 512x) = 19$, $v_2(128x\phi_2) = v_2(64x(\phi_2)^2) = v_2(32x(\phi_2)^3) = 17$, $v_2(20(\phi_2)^4) = 12$. Therefore, $N_2^-(f)$ has two sides of slopes -2 and $-5/3$:



Since both sides have degree one, the residual polynomials of second order have degree one: $R_{-2,2}(f)(y) = R_{-5/3,2}(f)(y) = y + 1$. Thus, both sides T_{-2} and $T_{-5/3}$ are terminal and the type $\mathbf{t}_1'$ branches into two f-complete types of order two:

$$\mathbf{t}_2 = (y; (x, -1/2, y+1); (\phi_2, -2, y+1)), \quad \mathbf{t}_2' = (y; (x, -1/2, y+1); (\phi_2, -5/3, y+1)).$$

They detect two prime ideals $\mathfrak{Q}$, $\mathfrak{Q}'$ with $e(\mathfrak{Q}/2) = f(\mathfrak{Q}/2) = 2$, $e(\mathfrak{Q}'/2) = 6$, $f(\mathfrak{Q}'/2) = 1$.

With respect to T_{-2}, we have $Q_{2,0} = Q_1$, $H_{2,0} = 15/2$, so that

$$\mathcal{B}_{T_{-2}} = Q_{2,0} \star \mathcal{B}_1 = \left\{ Q_1(\theta)/2^7, \, \theta Q_1(\theta)/2^8 \right\}.$$

With respect to $T_{-5/3}$, we have $Q_{2,0} = Q_4$, $H_{2,0} = 2$, $Q_{2,1} = Q_3$, $H_{2,1} = 23/6$, $Q_{2,2} = Q_2$, $H_{2,2} = 17/3$, so that

$$\mathcal{B}_{T_{-5/3}} = \bigcup_{0 \le j < 3} Q_{2,j} \star \mathcal{B}_1 = \left\{ \frac{Q_4(\theta)}{2^2}, \, \frac{\theta Q_4(\theta)}{2^2}, \, \frac{Q_3(\theta)}{2^3}, \, \frac{\theta Q_3(\theta)}{2^4}, \, \frac{Q_2(\theta)}{2^5}, \, \frac{\theta Q_2(\theta)}{2^6} \right\}.$$

The 2-integral basis $\mathcal{B} = \mathcal{B}_S \cup \mathcal{B}_{T_{-2}} \cup \mathcal{B}_{T_{-5/3}}$ is complete. The Hermite Normal Form algorithm transforms the basis into the following 12 integral elements:

$$1, \, \theta, \, \frac{\theta^2}{2}, \, \frac{\theta^3}{2}, \, \frac{\theta^4}{4}, \, \frac{\theta^5}{4}, \, \frac{\theta^6}{8}, \, \frac{\theta^7 + 8\theta}{16}, \, \frac{\theta^8 + 2\theta^6 + 8\theta^2 + 16}{32}, \, \frac{\theta^9 + 2\theta^7 + 8\theta^3 + 16\theta}{64},$$
$$, \frac{\theta^{10} + 12\theta^6 + 8\theta^4 + 96}{128}, \, \frac{\theta^{11} + 12\theta^7 + 8\theta^5 + 64\theta^3 + 224\theta}{256}.$$

References

[1] J.-D. Bauch, E. Nart, H. D. Stainsby, *Complexity of OM factorizations of polynomials over local fields*, LMS J. Comput. Math. **16** (2013), 139–171

[2] J. Buchmann, H.W. Lenstra, *Approximating rings of integers in number fields*, J. Théor. Nombres Bordeaux **6** (1994), 221–260.

[3] D. Ford, *The construction of maximal orders over a Dedekind domain*, J. Symb. Comput. **4**, (1987), 69–75.

[4] D. Ford, S. Pauli, X. Roblot, *A fast algorithm for polynomial factorization over $\mathbb{Q}_p$*, J. Théor. Nombres Bordeaux **14**, no. 1 (2002), 151–169.

[5] J. Guàrdia, J. Montes, E. Nart, *Okutsu invariants and Newton polygons*, Acta Arith. **145** (2010), 83–108.

[6] J. Guàrdia, J. Montes, E. Nart, *Higher Newton polygons in the computation of discriminants and prime ideal decomposition in number fields*, J. Théor. Nombres Bordeaux **23** (2011), no. 3, 667–696.

[7] J. Guàrdia, J. Montes, E. Nart, *Newton polygons of higher order in algebraic number theory*, Trans. Amer. Math. Soc. **364** (2012), no. 1, 361–416.

[8] J. Guàrdia, J. Montes, E. Nart, *A new computational approach to ideal theory in number fields*, Foundations of Computational Mathematics, DOI 10.1007/s10208-012-9137-5.

[9] J. Guàrdia, E. Nart, S. Pauli, *Single-factor lifting and factorization of polynomials over local fields*, J. Symb. Comput. **47** (2012), 1318–1346.
[10] E. Hallouin, *Computing local integral closures*, J. Symb. Comput. **32** (2001), 211–230.
[11] F. Hess, *Computing Riemann-Roch spaces in algebraic function fields and related topics*, J. Symb. Comput. **33** (2002), 425–445.
[12] M. van Hoeij, *A algorithm for computing an integral basis in an algebraic function field*, J. Symb. Comput. **18** (1994), 353–363.
[13] H. W. Lenstra, Jr., *Lattices*, pp. 127–181 in *Surveys in algorithmic number theory*, edited by J. P. Buhler and P. Stevenhagen, Math. Sci. Res. Inst. Publ. **44**, Cambridge University Press, New York, 2008.
[14] S. MacLane, *A construction for absolute values in polynomial rings*, Trans. Amer. Math. Soc. **40** (1936), 363–395.
[15] S. MacLane, *A construction for prime ideals as absolute values of an algebraic field*, Duke Math. J. **2** (1936), 492–510.
[16] K. Okutsu, *Construction of integral basis, I, II*, P. Jpn. Acad. A-Math. **58** (1982), 47–49, 87–89.
[17] Ø. Ore, *Bestimmung der Diskriminanten algebraischer Körper*, Acta Math-Djursholm **45** (1925), 303–344.
[18] Ø. Ore, *Newtonsche Polygone in der Theorie der algebraischen Körper*, Math. Ann. **99** (1928), 84–117.
[19] S. Pauli, *Factoring polynomials over local fields*, J. Symb. Comput. **32** (2001), 533–547.
[20] W. M. Schmidt, *Construction and estimation of bases in function fields*, J. Number Theory **39** (1991), 181–224.
[21] A. Schönhage, V. Strassen, *Schnelle Multiplikation groβer Zahlen*, Computing **7** (1971), 281–292
[22] M. Schörnig, *Untersuchungen konstruktiver Probleme in globalen Funktionenkörpern*, Dissertation Technische Universität Berlin, 1996.
[23] H. Zassenhaus, *Ein Algorithmus zur Berechnung einer Minimalbasis über gegebener Ordnung*, Funktionalanalysis, Approximationstheorie, Numerische Mathematik (Oberwolfach 1965), Birkhäuser, Basel, 1967, pp. 90–103.

Departament de Matemàtica Aplicada IV, Escola Politècnica Superior d'Enginyeria de Vilanova i la Geltrú, Av. Víctor Balaguer s/n. E-08800 Vilanova i la Geltrú, Catalonia, Spain

E-mail address: guardia@ma4.upc.edu

Departament de Ciències Econòmiques i Empresarials, Facultat de Ciències Socials, Universitat Abat Oliba CEU, Bellesguard 30, E-08022 Barcelona, Catalonia, Spain, Departament de Matemàtica Econòmica, Financera i Actuarial, Facultat d'Economia i Empresa, Universitat de Barcelona, Av. Diagonal 690, E-08034 Barcelona, Catalonia, Spain

E-mail address: montes3@uao.es, jesus.montes@ub.edu

Departament de Matemàtiques, Universitat Autònoma de Barcelona, Edifici C, E-08193 Bellaterra, Barcelona, Catalonia, Spain

E-mail address: nart@mat.uab.cat